Request for Proposal

STATE OF SOUTH DAKOTA
Bureau of Human Resources and Bureau of Financial Management
500 East Capitol Avenue
Pierre, South Dakota 57501-3182

State of South Dakota Infor HCM Implementation and Consulting Services
PROPOSALS ARE DUE NO LATER THAN: May 31, 2023, 4:00 PM CST

RFP #: 23RFP8552
BUYER: Bureau of Human Resources (BHR) and Bureau of Finance and Management (BFM)
EMAIL: Cole.Pry@state.sd.us

READ CAREFULLY

FIRM NAME:

ADDRESS:

CITY/STATE:

ZIP (9 DIGITS):

AUTHORIZED SIGNATURE:

TYPE OR PRINT NAME:

TELEPHONE NO:

FAX NO:

E-MAIL:

PRIMARY CONTACT INFORMATION

CONTACT NAME:

FAX NO:

TELEPHONE NO:

E-MAIL:

1 GENERAL INFORMATION

1.1 BIT STANDARD CONTRACT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include the State of South Dakota's (the "State") standard I/T contract terms listed in Appendix A, along with any additional contract terms as negotiated by the parties. As part of the negotiation process the contract terms listed in Appendix A may be altered or deleted. The offeror must indicate in its response any issues it has with specific contract terms. If the offeror does not indicate that there are any issues with any contract terms, then the State will assume those terms are acceptable to the offeror. There is also a list of technical questions, Security and Vendor Questions which is attached as Appendix B, the offeror must complete. These questions may be used in the proposal evaluation. It is preferred that the offeror's response to these questions is provided as a separate document from the RFP response. If the offeror will be hosting the solution, the file name must be "(Your Name) Hosted Security and Vendor Questions Response". If the solution will be hosted by the State, the file must be named "(Your Name) Security and Vendor Questions Response State Hosted". If the solution is not a hosted solution, the file name must be "(Your Name) Security and Vendor Questions Response". If there are multiple non-hosted solutions, please provide some designation in the file name that indicates which proposal it goes to. This document cannot be a scanned document but must be an original. If the offeror elects to make the Security and Vendor Questions part of its response, the questions must be clearly indicated in the proposal's Table of Contents. A single numbering system must be used throughout the proposal.

1.2 PURPOSE OF REQUEST FOR PROPOSAL (RFP)

The purpose of this RFP is to solicit proposals from qualified contractors to perform implementation and consulting services related to Infor CloudSuite HCM. Specifically, to perform the following projects:

- Migrate the state's Single-Tenant Infor HCM to Multi-Tenant, and perform business processes optimization to use the software more efficiently
- Implement multi-tenant payroll, replacing the state's current Lawson S3 V10 CloudSuite Public Sector, to V11 Payroll.
- Implement a Work Force Management (WFM) system. That includes timekeeping, scheduling and absence management to replace the state's current existing custom system.

1.3 ISSUING OFFICE AND RFP REFERENCE NUMBER

The State of South Dakota is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota, Bureau of Human Resources (BHR) and Bureau of Finance and Management (BFM). The reference number for the transaction is RFP# 23RFP8552. This number must be referred to on all proposals, correspondence, and documentation relating to the RFP.

1.4 LETTER OF INTENT

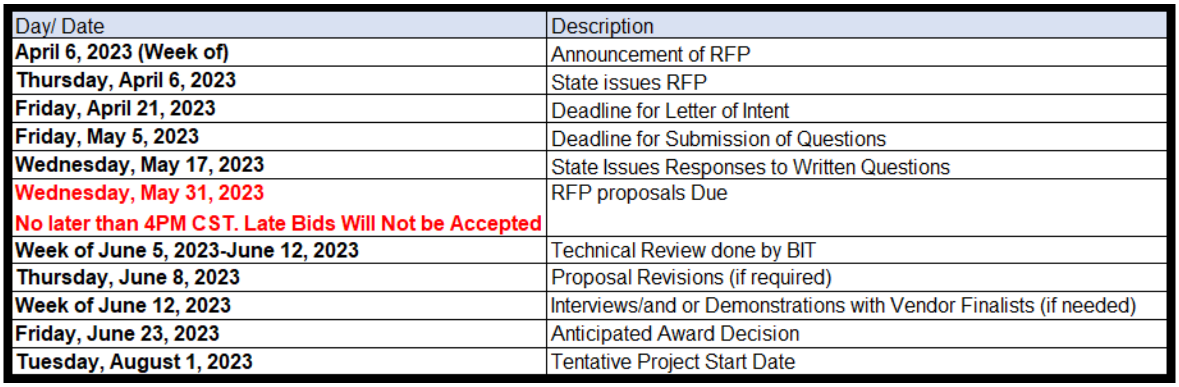
All interested offerors must submit a **Letter of Intent** to respond to this RFP.

The letter of intent must be received by the Bureau of Human Resources (BHR) no later than **April 21, 2023**, if submitting by mail the envelope should be addressed to:
Cole Pry/Bureau of Human Resources
The State of South
500 East Capitol
Pierre, SD 57501-3182

Be sure to reference the RFP number in your letter.

The Letter of Intent may be submitted to Bureau of Human Resources via email at cole.pry@state.sd.us. Please place the following in the subject line of your email: **“Letter of Intent for RFP# 23RFP8552”**.

1.5 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)



Day/ Date	Description
April 6, 2023 (Week of)	Announcement of RFP
Thursday, April 6, 2023	State issues RFP
Friday, April 21, 2023	Deadline for Letter of Intent
Friday, May 5, 2023	Deadline for Submission of Questions
Wednesday, May 17, 2023	State Issues Responses to Written Questions
Wednesday, May 31, 2023 **No later than 4PM CST. Late Bids Will Not be Accepted**	RFP proposals Due
Week of June 5, 2023-June 12, 2023	Technical Review done by BIT
Thursday, June 8, 2023	Proposal Revisions (if required)
Week of June 12, 2023	Interviews/and or Demonstrations with Vendor Finalists (if needed)
Friday, June 23, 2023	Anticipated Award Decision
Tuesday, August 1, 2023	Tentative Project Start Date

1.6 SUBMITTING YOUR PROPOSAL

All proposals must be completed and received in the Bureau of Human Resources (BHR) by the date and time indicated in the Schedule of Activities.

Proposals received after the deadline will be late and ineligible for consideration.

The State of South Dakota requires an original and three (3) copies along with electronic proposals via email. The RFP response sent via email should be sent unencrypted and be less than 20 MB. **The email subject line must include RFP #23RFP8552 and the Title.**

All proposals must be signed, in ink, by an officer of the offeror, legally authorized to bind the offeror to the proposal and sealed in the form. Proposals that are not properly signed may be rejected. The sealed envelope must be marked with the appropriate RFP Number and Title. The words “Sealed Proposal Enclosed” must be prominently denoted on the outside of the shipping container. **Proposals must be addressed and labeled as follows:**

REQUEST FOR PROPOSAL # 23RFP8552
PROPOSAL TITLE: INFOR HCM IMPLMENTATION AND CONSULTING SERVICES
PROPOSAL DUE: MAY 31, 2023, 4:00 PM CST
BUYER: Bureau of Human Resources (BHR) and Bureau of Finance and Management (BFM)
Attention: Cole Pry
Address: 500 East Capitol, Pierre, SD 57501-3182

No proposal shall be accepted from, or no contract or purchase order shall be awarded to any person, firm or corporation that is in arrears upon any obligations to the State of South Dakota, or that otherwise may be deemed irresponsible or unreliable by the State of South Dakota.

1.7 CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION – LOWER TIER COVERED TRANSACTIONS

By signing and submitting this proposal, the offeror certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation, by any Federal department or agency, from transactions involving the use of Federal funds. Where the offeror is unable to certify to any of the statements in this certification, the offeror shall attach an explanation to its offer.

1.8 NON-DISCRIMINATION STATEMENT

The State of South Dakota requires that all contractors, vendors, and suppliers doing business with any State agency, department, or institution, provide a statement of non-discrimination. By signing and submitting their proposal, the offeror certifies they do not discriminate in their employment practices with regard to race, color, creed, religion, age, sex, ancestry, national origin or disability.

1.9 RESTRICTION OF BOYCOTT OF ISRAEL

For contractors, vendors, suppliers, or subcontractors with five (5) or more employees who enter into a contract with the State of South Dakota that involves the expenditure of one hundred thousand dollars ($100,000) or more, by submitting a response to this solicitation or agreeing to contract with the State, the bidder or offeror certifies and agrees that the following information is correct:

The bidder or offeror, in preparing its response or offer or in considering proposals submitted from qualified, potential vendors, suppliers, and subcontractors, or in the solicitation, selection, or commercial treatment of any vendor, supplier, or subcontractor, has not refused to transact business activities, has not terminated business activities, and has not taken other similar actions intended to limit its commercial relations, related to the subject matter of the bid or offer, with a person or entity on the basis of Israeli national origin, or residence or incorporation in Israel or its territories, with the specific intent to accomplish a boycott or divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the bid or response submitted by the bidder or offeror on this project and terminate any contract awarded based on the bid or response. The successful bidder or offeror further agrees to provide immediate written notice to the contracting executive branch agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination.

1.10 RESTICTION OF PROHIBITED ENTITY

For contractors, vendors, suppliers, or subcontractors who enter into a contract with the State of South Dakota by submitting a response to this solicitation or agreeing to contract with the State, the bidder or offeror certifies and agrees that the following information is correct:

The bidder or offeror, in preparing its response or offer or in considering proposals submitted from qualified, potential vendors, suppliers, and subcontractors, or in the solicitation, selection, or commercial treatment of any vendor, supplier, or subcontractor, is not a prohibited entity, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela, as defined by South Dakota Executive Order 2023-02. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the bid or response submitted by the bidder or offeror on this project and terminate any contract awarded based on the bid or response. The successful bidder or offeror further agrees to provide immediate written notice to the contracting executive branch agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination.

1.11 MODIFICATION OR WITHDRAWAL OF PROPOSALS

Proposals may be modified or withdrawn by the offeror prior to the established due date and time.

No oral, telephonic, telegraphic or facsimile responses or modifications to informal, formal bids, or Request for Proposals will be considered.

1.12 OFFEROR INQUIRIES

All questions should be sent to: Cole.Pry@state.sd.us
Only emailed questions will be accepted.

Offerors that submitted a letter of intent may make email inquiries concerning this RFP to obtain clarification of requirements. No questions will be accepted after the date and time indicated in the above schedule of activities. Email inquiries must be sent to Cole Pry at Cole.Pry@state.sd.us with the subject line **“RFP# 23RFP8552**”. The Bureau of Human Resources and Bureau of Finance and Management prefer to respond to the offeror’s inquires (if required) via email. In addition, all inquiries and the State’s response will be posted on the state’s e-procurement system. The questions and their answers will be sent to all offerors that submitted Letters of Intent, submitted questions, or requested the questions and answers via email before the proposal submittal date and will be sent by the date and time indicated in the above calendar of events. Offeror may not rely on any other statements, either of a written or oral nature, that alter any specification or other term or condition of this RFP that have not originated from the SD

RFP Project Contact. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP.

1.13 PROPRIETARY INFORMATION

The proposal of the successful offeror(s) becomes public information. Proprietary information can be protected under limited circumstances such as client lists and non-public financial statements. An entire proposal may not be marked as proprietary. Offerors must clearly identify in the Executive Summary and mark in the body of the proposal any specific proprietary information they are requesting to be protected. The Executive Summary must contain specific justification explaining why the information is to be protected. Proposals may be reviewed and evaluated by any person at the discretion of the State. All materials submitted become the property of the State of South Dakota and may be returned only at the State's option.

1.14 LENGTH OF CONTRACT

The length of contract will be set by the scope and roadmap provided by the vendor and agreed upon by the State of South Dakota.

1.15 PRESENTATIONS/DEMONSTRATIONS

At its discretion, the State may require a presentation or demonstration by an offeror to clarify a proposal. However, the State may award a contract based on the initial proposals received without a presentation or demonstration by the offeror. If presentations or demonstrations are required, they will be scheduled after the submission of proposals. Presentations and demonstrations will be made at the offeror’s expense.

1.16 DISCUSSIONS

At the State’s discretion, the offeror may or may not be invited to have discussions with the State. The discussions can be before or after the RFP has been submitted. Discussions will be made at the offeror’s expense.

1.17 NEGOTIATIONS

This process is a Request for Proposal/Competitive Negotiation process. Each proposal shall be evaluated, and each respondent shall be available for negotiation meetings at the State’s request. The State reserves the right to negotiate on any component of every proposal submitted. From the time the proposals are submitted until the formal award of a contract, each proposal is considered a working document and as such, will be kept confidential. The negotiation discussions will also be held as confidential until such time as the award is completed.

2 STANDARD CONTRACT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include the State’s standard terms and conditions as listed below, along with any additional terms and conditions as negotiated by the parties. Please note additional terms and conditions may be required by the State.

2.1 The Contractor will perform those services described in the Scope of Work, attached hereto as Section 3 of the RFP and by this reference incorporated herein.

2.2 The Contractor's services under this Agreement shall commence and terminate on mutually agreed upon dates, unless terminated sooner pursuant to the terms hereof.

2.3 The Contractor will not use State equipment, supplies or facilities. The Contractor will provide the State with its Employer Identification Number, Federal Tax Identification Number or Social Security Number upon execution of this Agreement.

2.4 The State will make payment for services upon satisfactory completion of the services. The State will not pay Contractor's expenses as a separate item. Payment will be made pursuant to itemized invoices submitted with a signed state voucher. Payment will be made consistent with SDCL chapter 5-26.

2.5 The Contractor agrees to indemnify and hold the State of South Dakota, its officers, agents and employees, harmless from and against any and all actions, suits, damages, liability or other proceedings that may arise as the result of performing services hereunder. This section does not require the Contractor to be responsible for or defend against claims or damages arising solely from errors or omissions of the State, its officers, agents or employees. Contractor agrees to indemnify the State of South Dakota, its officers, agents, and employees, from and against all claims or proceedings for actions, suits, damages, liabilities, other losses or equitable relief that may arise at least in part as a result of an act or omission in performing services under this Agreement. Contractor shall defend the State of South Dakota, its officers, agents, and employees against any claim, including any claim, action, suit, or other proceeding related to the claim. Contractor's obligation to indemnify includes the payment of attorney fees and other costs of defense. In defending the State of South Dakota, its officers, agents, and employees, Contractor shall engage other professionals, subject to the written approval of the State which shall not be unreasonably withheld. Notwithstanding the foregoing, the State may, in its sole discretion and at the expense of Contractor, engage attorneys and other professionals to defend the State of South Dakota, its officers, agents, and employees, or to assist Contractor in the defense. This section does not require Contractor to be responsible for or defend against claims or proceedings for damages, liabilities, losses or equitable relief arising solely from errors or omissions of the State, its officers, agents or employees.

2.6 The Contractor, at all times during the term of this Agreement, shall obtain and maintain in force insurance coverage of the types and with the limits as follows:

A. Commercial General Liability Insurance:

Contractor shall maintain occurrence-based commercial general liability insurance or equivalent form of coverage with a limit of not less than one million dollars ($1,000,000) for each occurrence. If such insurance contains a general aggregate limit it shall apply separately to this Agreement or be no less than two times the occurrence limit. The insurance policy shall name the State of South Dakota, its officers and employees, as additional insureds, but liability coverage is limited to claims not barred by sovereign immunity. The State of South Dakota, its officers and employees do not hereby waive sovereign immunity for discretionary conduct as provided by law.

B. Professional Liability Insurance or Miscellaneous Professional Liability Insurance:
Contractor agrees to procure and maintain professional liability insurance or miscellaneous professional liability insurance with a limit not less than one million dollars ($1,000,000). The insurance policy shall name the State of South Dakota, its officers and employees, as additional insureds but liability coverage is limited to claims not barred by sovereign immunity. The State of South Dakota, its officers and employees do not hereby waive sovereign immunity for discretionary conduct as provided by law.

C. Business Automobile Liability Insurance:
Contractor shall maintain business automobile liability insurance or equivalent form with a limit of not less than one million dollars ($1,000,000) for each accident. This insurance shall include coverage for owned, hired and non-owned vehicles. The insurance policy shall name the State of South Dakota, its officers and employees, as additional insureds but liability coverage is limited to claims not barred by sovereign immunity. The State of South Dakota, its officers and employees do not hereby waive sovereign immunity for discretionary conduct as provided by law.

D. Worker's Compensation Insurance:
Contractor shall procure and maintain workers' compensation and employers' liability insurance as required by South Dakota or federal law.

Before beginning work under this Agreement, Contractor shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement including naming the State, its officers and employees, as additional insureds, as set forth above. In the event of a substantial change in insurance, issuance of a new policy, cancellation or nonrenewal of the policy, Contractor agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required. Contractor shall furnish copies of insurance policies if requested by the State.

2.7 While performing services hereunder, the Contractor is an independent contractor and not an officer, agent, or employee of the State of South Dakota.

2.8 Contractor agrees to report to the State any event encountered in the course of performance of this Agreement which results in injury to the person or property of third parties, or which may otherwise subject Contractor or the State to liability. Contractor shall report any such event to the State immediately upon discovery.

2.9 Contractor's obligation under this section shall only be to report the occurrence of any event to the State and to make any other report provided for by their duties or applicable law. Contractor's obligation to report shall not require disclosure of any information subject to privilege or confidentiality under law (e.g., attorney-client communications). Reporting to the State under this section shall not excuse or satisfy any obligation of Contractor to report any event to law enforcement or other entities under the requirements of any applicable law.

2.10 This Agreement may be terminated by either party hereto upon thirty (30) days written notice. In the event the Contractor breaches any of the terms or conditions hereof, this Agreement may be terminated by the State at any time with or without notice. If termination for such a default is affected by the State, any payments due to Contractor at the time of termination may be adjusted to cover any additional costs to the State because of Contractor's default. Upon termination the State may take over the work and may award another party an agreement to complete the work under this Agreement. If after the State terminates for a default by Contractor it is determined that Contractor was not at fault, then the Contractor shall be paid for eligible services rendered and expenses incurred up to the date of termination.

2.11 This Agreement depends upon the continued availability of appropriated funds and expenditure authority from the Legislature for this purpose. If for any reason the Legislature fails to appropriate funds or grant expenditure authority, or funds become unavailable by operation of law or federal funds reductions, this Agreement will be terminated by the State. Termination for any of these reasons is not a default by the State nor does it give rise to a claim against the State.

2.12 This Agreement may not be assigned without the express prior written consent of the State. This Agreement may not be amended except in writing, which writing shall be expressly identified as a part hereof and be signed by an authorized representative of each of the parties hereto.

2.13 This Agreement shall be governed by and construed in accordance with the laws of the State of South Dakota. Any lawsuit pertaining to or affecting this Agreement shall be venued in Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

2.14 The Contractor will comply with all federal, state and local laws, regulations, ordinances, guidelines, permits and requirements applicable to providing services pursuant to this Agreement, and will be solely responsible for obtaining current information on such requirements.

2.15 The Contractor may not use subcontractors to perform the services described herein without the express prior written consent of the State. The Contractor will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Agreement, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this Agreement. The Contractor will cause its subcontractors, agents, and employees to comply, with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements and will adopt such review and inspection procedures as are necessary to assure such compliance.

2.16 Contractor hereby acknowledges and agrees that all reports, plans, specifications, technical data, miscellaneous drawings, software system programs and documentation, procedures, or files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, and all information contained therein provided to the State by the Contractor in connection with its performance of services under this Agreement shall belong to and is the property of the State and will not be used in any way by the Contractor without the written consent of the State. Papers, reports, forms, software programs, source code(s) and other material which are a part of the work under this

Agreement will not be copyrighted without written approval of the State.

2.17 The Contractor certifies that neither Contractor nor its principals are presently debarred, suspended, proposed for debarment or suspension, or declared ineligible from participating in transactions by the federal government or any state or local government department or agency. Contractor further agrees that it will immediately notify the State if during the term of this Agreement Contractor or its principals become subject to debarment, suspension or ineligibility from participating in transactions by the federal government, or by any state or local government department or agency.

2.18 Pursuant to South Dakota Executive Order 2023-02, by entering into this Agreement with the State of South Dakota, the Contractor certifies and warrants that the Contractor is not a prohibited entity, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela, as defined by South Dakota Executive Order 2023-02.

The Contractor agrees that if this certification is false, the State may terminate this Agreement with no further liability to the State. The Contractor further agrees to provide immediate written notice to the State if during the term of the contract it no longer complies with this certification, and the Contractor agrees such noncompliance may be grounds for contract termination.

2.19 Any notice or other communication required under this Agreement shall be in writing and sent to the address set forth above. Notices shall be given by and to Darin Seeley on behalf of the State, and by and to ___________, on behalf of the Contractor, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

2.20 In the event that any court of competent jurisdiction shall hold any provision of this Agreement unenforceable or invalid, such holding shall not invalidate or render unenforceable any other provision hereof.

2.21 All other prior discussions, communications and representations concerning the subject matter of this Agreement are superseded by the terms of this Agreement, and except as specifically provided herein, this Agreement constitutes the entire agreement with respect to the subject matter hereof.

3 SCOPE OF WORK

The intent of this request is to obtain a contract to perform implementation and consulting services for our current GHR to Multi-Tenant CloudSuite, including Core, Benefits Management, Talent Acquisition, Candidate Self Service, and Performance Management. The current Lawson S3 Payroll to V11 Payroll, Symmetry, I-9 tracker configuration, and the implementation of a Work Force Management system. The goal of the completed project is to substantially improve the ability to provide timely and accurate Human Resource Support via improved processes and optimized use of technology. The project must be guided by the goal to reduce or eliminate low to no-value added work and improve the quality of data by leveraging automation, workflows, reporting, manager and self-service functionality and utilization. Additional business objectives are:

- Streamlining integration between internal and third-party systems to gain efficiency, timeliness, and quality data control.
- Delivering self-service reporting to leadership across state government to access the data needed for decision making.
- Reduce or eliminate manual processes, including removal of paper forms and manual workflow routing.
- Increase data analytics to provide timely access to information for State of South Dakota agencies.

3.1 Scope of Services and Tasks

The contractor shall provide services and deliverables as set forth in the tasks below, including a project plan and road map to accomplish each of the following:

3.1.1 Migrate the state's Single-Tenant Infor Global Human Resources (GHR) instance to multi-Tenant CloudSuite by providing technical and production support to implement and optimize best practices in the following areas:

3.1.1.1 Core HR
3.1.1.2 Employee and Manager Space
3.1.1.3 Benefits
3.1.1.4 Talent and Recruiting
3.1.1.5 Configuration Hiring Workflow
3.1.1.6 Employee Transition
3.1.1.7 Performance Management
3.1.1.8 Mobile capabilities

3.1.2 Replace Lawson S3 Payroll with HCM V11 Multi-Tenant payroll by providing technical and production support to implement and optimize best practices, including data migration conversion.

3.1.3 Implementation of Symmetry and I-9 Tracker to replace current business process and optimize best practices.

3.1.4 Implementation of a Workforce Management solution to replace the state's custom time keeping system and multiple agencies owned scheduling platforms.

3.1.4.1 Labor Scheduling and Forecasting
3.1.4.2 Absences Management (2 accrual rates per leave)
3.1.4.3 Time and Labor Rules/Time Study Rules
3.1.4.4 Workflow Approvals
3.1.4.5 Timesheets
3.1.4.6 Mobile capabilities

3.1.5 Queries and Reports - collaborate with the State to develop queries and reports using personalization, Power BI, MS Query, and dashboards. These must be reliable, efficient, and effective to meet the business needs.

3.1.5.1 Reporting Tools, Data Cubes, Dashboards training
3.1.5.2 Reporting Tools Configuration

3.1.5.3 Functional Security Overview training
3.1.5.4 Functional and Technical Design
3.1.5.5 Develop Reports
3.1.5.6 Unit Testing

The contract doubles as an agreement for the State to own the data tables and is able to manipulate data, run reports as needed, pull code tables, access raw data, and develop dashboards as needed through Microsoft Power BI, ESRI, Tableau and associated platforms.

3.1.6 Integrations - develop integrations with internal and external systems to specifications. Monitor scheduled jobs, processes, work units, BOD's, and system interfaces with Async.

As part of the State's Identity and Access Management (IAM) strategy, the solution will need to integrate with the State of South Dakota's standard identity management service single sign-on (SSO) which enables custom control of how citizens and state employees sign up, sign in, and manage their profiles.

The SSO supports two industry standard protocols: OpenID Connect and OAuth 2.0 (preferred). This identity management will handle password recovery. Multi-factor Authentication (MFA) is required for all application Administrators and may be required for other users. Microsoft's official documentation on the identity provider the State has implemented can be found at https://docs.microsoft.com/en-us/azure/active-directory-b2c/ and https://docs.microsoft.com/en-us/azure/active-directory-b2c/integrate-with-app-code-samples.

If the offeror is not able to fulfill this identity management standard, they will be excluded from the list.

3.1.7 Configurations and Interfaces – In the case there are configurations needed the requirement would be to design, develop, test, debug, and deploy business configuration and interfaces requirements according to specifications to meet requirements by using Configuration Console, and IPA. The business interfaces and configurations need to be reliable, efficient, and effective.

The offeror must also describe how the system can adapt to business necessary interfaces using widely adopted open APIs and standards. Additionally, BHR and BFM expects the offeror will make available/expose software services and publish documentation for those software services that would enable third party developers to interface other business applications. A detailed description of system capability shall be included in the proposal.

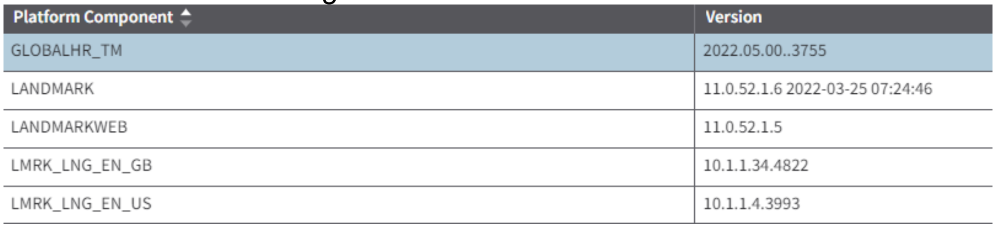
3.1.8 Review and Testing - assist in the review and testing by providing effective and efficient support during the reviewing, updating, and testing phases of the project.

3.2 Expectations

The State desires to engage with a consultant/implementation partner with product expertise, to assist the State's project team to make best-practice decisions that the State can accept and implement. The consultant will provide Infor product expertise, project management, system configuration, reporting, integration development and support to the State's project team which includes members from the Bureau of Finance and Management, Bureau of Human Resources, and Bureau of Information and Telecommunications. The State of South Dakota requires a description of implementation methodology and timeline, the vendor roles and responsibilities, the client roles and responsibilities, the keys to a successful implementation, best practices used by the vendor, and the vendor's support model. The scope of this project includes assessing and analyzing the current state for business optimization, developing a strategic project timeline and implementation plan. Deliverables must include a project plan, assessment for business optimization, stakeholder assessment, gap analysis and a detailed roadmap as part of the proposal.

3.3 Current Environment

The State is currently on GHR Single-Tenant CloudSuite for Human Resources, Benefits, Performance Management, and Talent Acquisition. Our current versions are shown below for GHR Single-Tenant:



Platform Component	Version
GLOBALHR_TM	2022.05.00..3755
LANDMARK	11.0.52.1.6 2022-03-25 07:24:46
LANDMARKWEB	11.0.52.1.5
LMRK_LNG_EN_GB	10.1.1.34.4822
LMRK_LNG_EN_US	10.1.1.4.3993

The State is in S3 for payroll, which is CloudSuite. The S3 Version we are on is Infor Lawson 10.1.0.31.2011. The State is migrating from GHR CloudSuite Single-Tenant to Multi-Tenant with Infor for Benefits, Performance Management, Talent and to V11 Payroll. The State currently has a homegrown Time and Attendance program called TKS, which is on premise. The State is aware that there are many opportunities for process improvements/business optimization during this project.

The State has two primary HR organizations. The first organization has approximately 8000 state employees who are paid from S3 payroll and are in GHR for benefits. The Core HR system of record is GHR. The second HR organization pays approximately 4000 board of regent's employees within their own system, not S3. However, those 4000 employees are in GHR for benefits.

3.4 Requirements

The requirement of this request is to begin by performing a migration of the state's Single-Tenant Infor Global Human Resources (GHR) instance to multi-Tenant

CloudSuite by providing technical and production support optimize best practices and provide implantation services as indicated in the following areas:

3.4.1 Migration and audit of Performance Appraisals and Check Ins including, but not limited to, configurations, workflow approvals and reporting capabilities;

3.4.2 Implementation of payroll including, but not limited to, configuration of pay frequency, earning codes, deduction codes, tax jurisdictions, banks for payroll payments, tax withholding, pay calendars, semi-monthly payroll runs, correction runs, misc. payroll runs, pay periods, unemployment insurance rates, salary basis, departments, garnishments, retro pay elements, payment methods, developed check writer and printed pay slips, self-service direct deposit and W4 changes, and view pay slips;

3.4.3 Implementation of a Workforce Management System including, but not limited to, the absence types, absence reasons, absence plans, approval rules, and configuration of leave balances. This will also include time and labor rules and schedules built for several different time studies to accommodate multiple agencies;

3.4.4 Migration and audit of Benefits, including but not limited to configuration of benefit programs, benefit plans, eligibility profiles, life events, self-service benefits, open enrollment, interfaces to vendors through automation, and 1095C process and best practices;

3.4.5 Implementation of Transitions and Recruiting including but not limited to applicant tracking system, new hire onboarding and automation, transfers, configuration of new hire forms, workflows, offboarding, reporting, and metrics;

3.4.6 Migration of Employee and Manager Space to provide a better user experience for managers and employees;

3.4.7 Implementation of security including, but not limited to, role-based security and auditing;

3.4.8 Implementation of Interfaces and Integrations including outbound, inbound, and internal. There could be some interfaces that are high in complexity and may require the following: complex field mapping and data translation; complex conditions and/or data transformation; complex programing, including web services, batch jobs, updates for Infor security. This will also include any new interfaces that are needed:

3.4.8.1 Define Interface Strategies and Requirements
3.4.8.2 Functional and Technical Design Specifications
3.4.8.3 Develop Interface and test scripts
3.4.8.4 Testing of Interfaces

3.4.9 Data conversion to include at least one year of historical data into Multi-Tenant from S3 Payroll and applicant data in GHR and S3, will be decided between vendor and the State. All other historical data will be converted into a data lake/data warehouse. The vendor will be required to perform all conversion iterations required to ensure that all data is converted accurately. Pricing should not assume a limited number. The State and the vendor will agree upon the number of conversions required to ensure a successful HCM migration. Conversion activities will include the following:

3.4.9.1 Planning
3.4.9.2 Data Clean Up and Mapping
3.4.9.3 Data Validation Preparation
3.4.9.4 Data Extract, Transformation and Load
3.4.9.5 Data Conversion (SIT, UAT, PROD)

3.4.10 Data Migration to include efforts associated with historical data from prior Infor systems into current Infor systems through the Data Migration Factory;

3.4.11 Implementation of reports to include new or redeveloped reports if necessary;

3.4.12 System training for the project team on the system architecture, system design, and module specific processing;

3.4.13 Overall training services to include the following:

3.4.13.1 Instructor led courses online or onsite
3.4.13.2 Courses should be tailored to respective areas
3.4.13.3 Training materials tailored to the State's processes
3.4.13.4 Production of all training materials electronically
3.4.13.5 Scheduling of training classes
3.4.13.6 Surveys for training feedback
3.4.13.7 Data preparation
3.4.13.8 Job aids and quick reference guides
3.4.13.9 Recording of training sessions

3.4.14 Review and revise business process documentation to ensure consistency and best business practices;

3.4.15 Replacement of selected existing customization and modifications with delivered functionality;

3.4.16 Implementation of any additional features or customizations available that are not being utilized by the State currently;

3.4.17 Development of testing plans and guidance to the State in creating test scripts. Provide a detailed comprehensive functional and technical test plan/script to include the following:

3.4.17.1 Scripts for each functional area
3.4.17.2 Integration test plans including end to end process
3.4.17.3 Parallel test plans to include validation tools
3.4.17.4 Conversation Test Plan

3.4.18 Provide State with Testing/Acceptance Plan. The vendor must test all configurations, modifications, interfaces, and data conversations prior to turning over to the State for testing. The vendor should provide the following:

3.4.18.1 System Test plan

3.4.18.2 Parallel Test plan
3.4.18.3 User Acceptance Test Plan

3.4.19 Define and provide a plan for post Go Live support that ensures that official business systems are supported during normal business hours as well as response times to critical issues. This should not last longer than 90 days after go live date;

3.4.20 Documentation of all system changes and configurations;

3.4.21 Provide a full detail requirement list to include gap analysis documentation and migration plan;

3.4.22 Provide the state with organizational change management to include the following:
3.4.22.1 Analyze business process impacts.
3.4.22.2 Compare current to future processes to determine impact.
3.4.22.3 Confirm alignment with the State of South Dakota.
3.4.22.4 Develop an action plan/road map by department and functional areas to prepare for impact.
3.4.22.5 Provide overall project communication services through multiple channels to ensure effectiveness for each phase of the project to include the following:
3.4.22.5.1 Talking Points
3.4.22.5.2 Fact Sheets
3.4.22.5.3 FAQ

4 VENDOR QUALIFICATIONS AND REQUIREMENTS

4.1 Description of Organization

Provide a brief description of your organization and background, including the number of years in business, number of employees, and ability to provide the required services outlined in the RFP. Please include specifics related to public sector expertise, focus, and implementation.

4.2 Project Organization Chart

List names, job titles (designate vacancies), and the city and state in which individual will work on this project. List all entities to be used for performance of the services described in this RFP. In the work plan, describe which responsibilities will be assigned to consultants or subcontractors and the city and state in which the consultants or subcontractors are located.

4.3 Qualifications and Experience

Describe how appropriate consultant staff will be identified and assigned to the State of South Dakota for each of the project deliverables. Please include qualifications, certifications, and experience of personnel and or subcontractors. Please clearly associate specific staff to work tasks and estimate the percentage of time they will be available for the project**.**

4.4 Staff Resumes and References

Resumes and references of key personnel, key personnel are considered to be those who are accountable for the completion of one or more major deliverables, has the responsibility of any or all of the total project management, or is responsible for the completion of the project. Provide resume details for all key personnel, including any subcontractors' project leads, by listing the following in the order in which it appears.

- Name
- Title
- Contact Information (telephone number(s), e-mail address)
- Work Address
- Project Responsibilities (as they pertain to this project)
- Percentage of time designated to this project
- Brief listing of work experience in reverse chronological order from present to 2013 (only provide company name, job title(s)/position(s) held, date started, and date left each position, brief description of job duties, responsibilities, and significant accomplishments)
- RFP Project Experience
- Technical Background relative to this project
- Experience in Similar Projects
- Names of the Similar Projects they were involved in
- Role they played in the projects similar to this project
- Project Management Experience
- Technical Knowledge
- Education
- Relevant Certifications
- Three Professional References (name, telephone number, company name, relationship to employee)

5 TECHNICAL APPROACH/WORK PLAN/PROJECT DELIVERABLES

5.1 Technical Approach

Describe your approach to completing the Scope of Services. Identify deliverables and key decision points. Provide comments regarding the proposed scope. The proposal should address specifically each of the following elements: Capability, Capacity and Qualification. Provide detailed description of the vendors organization including unique strengths, skills, capabilities, and experience consultants would bring to the project staffing Plan. Provide a proposed staffing plan for this project. The staffing plan should include the roles, and % FTE/time allocated by each staff member. Please identify the project manager for this project and all leads for this project provided by the consultant.

5.2 Work Plan

Describe in detail the framework within which the requested roadmap and implementation plan will be developed and provide a proposed work plan with the timelines carrying out this work. The proposed work plan shall clearly associate specific staff to the major tasks listed in the scope and estimate the percentage of time staff will be available to the project. To illustrate your work plan/strategy describe tools and techniques you will use, and identity challenges you anticipate when addressing specific requirements as identified in the scope. It may suggest modifications to the scope which may be considered for incorporation into the final contract. Modifications should be included in subtasks to the most appropriate task in the outline. The vendor should discuss the specific process and activities they will do to complete the following work:

5.2.1 Stakeholder engagement. The work plan should include details of how the consultant will engage with the stakeholders.

5.2.2 Gap analysis. The work plan should include detail about the type of gaps that will be included in the analysis and how the consultant will identify those gaps.

5.2.3 Roadmap. The work plan should address specifically how the roadmap will be developed, how the consultant intends to work with the stakeholders to establish priorities.

5.2.4 Implementation plan. The work plan should include how the consultant plans to develop the implementation plan, including the process use to develop specific objectives, activities, timeframes, as well as identifying and getting buy in.

5.2.5 Staffing (FTE) Matrix. The work plan should include a matrix of personnel tasks and estimate effort in hours for both the consultants and the required personnel tasks and estimate of hours by the State

5.3 Approach/Methodology

Define the general approach and specific methodology the consultant will take conducting a Roadmap. Discuss if this methodology has been used in the past, weather there has been difficulties or challenges in using the proposed approach and if so, how the consultant overcame those. Identify the what the consultant thinks the biggest risks to this project are and what approaches the consultant used to identify, address, and mitigate the risks.

5.4 Litigation, Audits, and Investigations

Describe any pending, concluded or threatened litigation, administrative proceedings or federal or state investigations or audits, subpoenas, or other information requests of or involving your firm or owners, principals or employees of your firm during the period beginning January 1, 2010, to present. Describe the nature and status of each matter and the resolution, if concluded. Please describe any potential conflicts that may affect your service to the State of South Dakota if applicable

5.5 Client References

5.5.1 Provide a list of all the firm’s clients comparable to the to the State indicating the length of service for each account. The State of South Dakota may contact and/or visit any of these accounts.

5.5.2 For each part of the project, provide a project description, project costs, dates of engagement, project owner, and member(s) of the proposed team for this RFP who participated in the project, including subcontractors.

5.5.3 For each reference, provide the contact person's name, title, address, phone number, e-mail address. Please ensure that the contact information is accurate for each reference.

5.6 Infor Partner

All Proposers must be Infor Partners. Please submit proof of partnership.

5.7 Pricing Information

Pricing is a factor in the selection. It is the Proposer's responsibility to state all pricing and/or costs associated with the proposal that is necessary to provide the services outlined in this RFP. Cost/Pricing information is to be included as part of the proposal as follows in a detailed breakdown:

5.7.1 Direct Labor Cost (Direct Labor Rates are based on a normal 8-hour day, 40 hours per week)

5.7.2 Consultants and key subcontractor schedule of fringe benefits and general overhead showing title/description of each indirect costs account and individual percentage for each account adding up to the total percentage for fringe benefits and general overhead.

5.7.3 Other Direct Costs and their basis.

5.7.4 Professional Fees.

5.7.5 Labor Multiplier.

5.7.6 Fully Loaded Hourly Rate.

5.7.7 Unit Rates, if applicable.

5.7.8 Proposed Total Amount

5.8 Bureau of Information (BIT) Requirements

The offeror must provide a diagram giving an overview of the proposed system. It is preferred that this diagram be provided as a separate document or attachment. The file must be named "(Your Name) Hosted System Diagram". If the offeror elects to make the diagram part of the proposal, then the location of the diagram must be clearly indicated in the Table of Contents.

The offeror should state whether its proposed solution will operate in a virtualized environment. Offeror also should identify and describe all differences, restrictions or limitations of its proposed solution with respect to operation, licensing, support, certification, warranties, and any other details that may impact its proposed solution when hosted in a virtualized environment. This information must be included with the solution diagram for the offeror hosted solution.

This section identifies tasks and deliverables of the project as described in Section 3 above. The selected offeror is responsible for providing the required deliverables. These deliverables will be the basis against which the offeror's performance will be evaluated.

The offeror is required to include a test system for its application. This test system will be used at the discretion of BIT. All resource costs associated with keeping the test system available must be borne by the project owner or the offeror. Any licensing costs for the test system must be included with the costs.

At BIT's discretion, any code changes made by the offeror, either during this project or thereafter, will be placed in the above test system first. It is at BIT's discretion if the code changes are applied by BIT or the offeror. If the code testing delays a project's timeline, a change management process should be followed, and the State will not be charged for this project change. If the test and production systems are to be hosted by the State, the schedule for the testing of the code changes is to be decided by BIT. Testing of emergency code changes will be scheduled by BIT based on the severity and resource availability.

The test system will be maintained by the offeror as a mirror image of the production system code base. At BIT's discretion, updates to the production system will be made by copying code from the test system after the test system passes BIT certification requirements.

If BIT determines that the application must be shut down on the production system, for any reason, the offeror will, unless approved otherwise by BIT, diagnosis the problem on and make all fixes on the test system. The offeror is expected to provide proof, to BIT, of the actions taken to remediate the problem that led to the application being denied access to the production system before the application can go back into production. This proof can be required by BIT even if the fix passes all BIT certification criteria. BIT is willing to sign a non-disclosure agreement with the offeror if the offeror feels that revealing the fix will put the offeror's intellectual property at risk.

All solutions acquired by the State that are hosted by the offeror, including Software as a Service, or hosted by a third-party for the offeror will be subjected to security scans by BIT or preapproved detailed security scan report provided by the offeror. The scan report sent in with the proposal can be redacted by the offeror. The State's goal at this point is to see if the contents of the report will be acceptable, not to review the contents themselves. If the offeror will be providing a security scan report, one must be sent with the proposal for approval. Approval is not guaranteed. If the scan report is not acceptable, the State must scan the offeror's solution. The actual scanning by the State or the submission of a security scan report will be done if the proposal is considered for further review. A detailed security report must consist of at least:

- The system that was evaluated (URL if possible, but mask it if needed).
- The categories that were evaluated (example: SQL injection, cross site scripting, etc.)
- What were the general findings, (meaning how many SQL injection issues were found, what was the count per category)
- Technical detail of each issue found. (Where was it found – web address, what was found, the http response if possible)

The cost of any scans done by the offeror or the offeror's costs associated with the State's scans must be part of the offeror’s bid. If the offeror is sending a security scan report, it should price the product both as if the State was to do the security scan or if the offeror was to do the security scan.

All hardware, website(s), or software purchased by the State and hosted by the State will be subjected to security scans by BIT.

Security scanning will be performed during the software development phase and during pre-production review. These scans and tests can be time consuming and should be allowed for in project planning documents and schedules. Products that do not meet BIT’s security and performance requirements will not be allowed to go into production and may be barred from UAT until all issues are addressed to the State’s satisfaction. The State urges the use of industry scanning/testing tools and secure development methods be employed to avoid unexpected costs and project delays. Costs to produce and deliver secure and reliable applications are the responsibility of the software entity producing or delivering an application to the State. Unless expressly indicated in writing, the State assumes all price estimates and bids are for the delivery and support of applications and systems that will pass security and performance testing. If the State determines the hardware, website(s), software, and or cloud services have security vulnerabilities that must be corrected, the State will inform the offeror of the nature of the issue and the offeror will be required to respond in writing regarding mitigation plans for the security vulnerabilities. If the product(s) does not pass the initial security scan, additional security scans may be required to reach an acceptable level of security. The offeror must pass a final follow-up security scan for the website(s), software or cloud services for the product(s) to be acceptable products to the State. The State may suspend or cancel payments for hardware, website(s), software, or cloud services that do not pass a final security scan.

Any website or web application hosted by the offeror that generates email cannot use “@state.sd.us” as the originating domain name per state security policy.

As part of this project, the offeror will provide a monitoring tool the State can utilize to monitor the operation of the proposed solution as well as all systems and all subcomponents and connections. It is required that this tool be easy to use and provide a dashboard of the health of the proposed solution. The effectiveness of this monitoring tool will be a component of the acceptance testing for this project.

As part of the project plan, the offeror will include development of an implementation plan that includes a back out component. Approval of the implementation plan by BIT should be a project milestone. Should the implementation encounter problems that cannot be resolved and the implementation cannot proceed to a successful conclusion, the back out plan will be implemented. The Implementation and back out documentation will be included in the project documentation.

The successful offeror will use the approved BIT processes and procedures when planning its project, including BIT’s change management process. Work with the respective agency’s BIT Point of Contact on this form. The Change Management form is viewable only to BIT employees. The purpose of this form is to alert key stake holders (such as: Operations, Systems Support staff, Desktop Support staff, administrators, Help Desk personnel, client representatives, and others) of changes that will be occurring within state resources and systems to schedule the:

- Movement of individual source code from test to production for production systems
- Implementation of a new system
- A major enhancement to a current system or infrastructure changes that impact clients
- Upgrades to existing development platforms

If as part of the project the state will be acquiring software the proposal should clearly state if the software license is perpetual or a lease. If both are options, the proposal should clearly say so and state the costs of both items separately.

Include in your submission details on your:

- Data loss prevention methodology;
- Identity and access management;
- Security intelligence;
- Annual security training and awareness;
- Manual procedures and controls for security;
- Perimeter controls;
- Security certifications and audits.

If the offeror will have State data on its system(s) or on a third-party's system and the data cannot be sanitized at the end of the project, the offeror's proposal must indicate this and give the reason why the data cannot be sanitized as per the methods in NIST 800-88.

The offeror's solution cannot include any hardware or hardware components manufactured by Huawei Technologies Company or ZTE Corporation or any subsidiary or affiliate of such entities. This includes hardware going on the State's network as well as the offeror's network if the offeror's network is accessing the State's network or accessing State data. This includes Infrastructure as a Service, Platform as a Service or Software as a Service situations. Any company that is considered to be a security risk by the government of the United States under the International Emergency Economic Powers Act, in a United States appropriation bill, an Executive Order, or listed on the US Department of Commerce's Entity List will be included in this ban.

If the offeror's solution requires accounts allowing access to State systems, then the offeror must indicate the number of the offeror's staff or subcontractors that will require access, the level of access needed, and if these accounts will be used for remote access. These individuals will be required to use Multi-Factor Authentication (MFA). The State's costs in providing these accounts will be a consideration when assessing the cost of the offeror's solution. If the offeror later requires accounts that exceed the number of accounts that was originally indicated, the costs of those accounts will be borne by the offeror and not passed onto the State. All State security policies can be found in the Information Technology Security Policy (ITSP) attached to this RFP. The offeror should review the State's security policies regarding authorization, authentication, and, if relevant, remote access (See ITSP 230.67, 230.76, and 610.1). Use of Remote Access Devices (RAD) by contractors to access the State's system must be requested when an account is requested. The offeror should be aware that access accounts given to non-state employees, Non-State (NS) accounts, will be disabled if not used within 90 days. An NS account will be deleted after Y days if it is not used.

Testing: If the software is being hosted on the state systems, regression testing, and integration testing is done by the contractor with assistance of BIT Development. If the software is being hosted on the state systems, functional testing is generally done by the contractor and the agency with assistance of BIT Development. If the software is being hosted on the state systems, performance testing and load testing is generally done by BIT Telecommunications division. If the contractor is hosting the software on its systems, regression testing, if relevant, integration testing, if relevant, functional testing, performance and load testing should be done by the contractor. The UAT is generally done by the contractor and the agency, whether the software is hosted on the State's or the contractor's systems. All testing is done in test environments either set up by the contractor or by BIT. All test results should meet the requirements of the agency before the software goes into production. For a software development project when the software is being customized, at a minimum, regression, integration, functional, and UAT tests must be done. If software is being developed fresh, at a minimum, integration, functional, and UAT tests must be done. How extensive the testing would be could vary with the criticality or complexity of an application. If you are unsure of the types of testing that should be done, bring the question up at the client planning meeting for the RFP. If performance and load tests are not done, then you are accepting the risk that your application may not perform as fast, do the amount of work you would like, or not operate under all the conditions you would want. Assuming no problems are found, you should plan on a minimum of three weeks for performance and load testing if done by BIT. There have been contractors on major projects that have had the attitude that if a project falls behind, the best way to make up the time is to reduce the testing, most commonly the performance and load testing. Be aware of the risks you run if this is proposed to you.

Regression Testing- Regression testing is the process of testing changes to computer programs to make sure that the older programming still works with the new changes.

Integration Testing- Integration testing is a software development process which program units are combined and tested as groups in multiple ways. In this context, a unit is defined as the smallest testable part of an application. Integration testing can expose problems with the interfaces among program components before trouble occurs in real-world program execution. Integration testing is also known as integration and testing (I&T).

Functional Testing- Functional testing is primarily used to verify that a piece of software is meeting the output requirements of the end-user or business. Typically, functional testing involves evaluating and comparing each software function with the business requirements. Software is tested by providing it with some related input so that the output can be evaluated to see how it conforms, relates or varies compared to its base requirements. Moreover, functional testing also checks the software for usability, such as ensuring that the navigational functions are working as required. Some functional testing techniques include smoke testing, white box testing, black box testing, and unit testing.

Performance Testing- Performance testing is the process of determining the speed or throughput of an application. This process can involve quantitative tests such as measuring the response time or the number of MIPS (millions of instructions per second) at which a system functions. Qualitative attributes such as reliability, scalability and interoperability may also be evaluated. Performance testing is often done in conjunction with load testing.

Load Testing- Load testing is the process of determining the ability of an application to maintain a certain level of effectiveness under unfavorable conditions. The process can involve tests such as ramping up the number of users and transactions until the breaking point is reached or measuring the frequency of errors at your required load. The term also refers to qualitative evaluation of factors such as availability or resistance to denial-of-service (DoS) attacks. Load testing is often done in conjunction with the more general process of performance testing. Load testing is also known as stress testing.

User Acceptance Testing- User acceptance testing (UAT) is the last phase of the software testing process. During UAT, actual software users test the software to make sure it can handle required tasks in real-world scenarios, according to specifications. UAT is one of the final and critical software project procedures that must occur before newly developed or customized software is rolled out. UAT is also known as beta testing, application testing or end user testing. In some cases, UAT may include piloting of the software.

The State, at its sole discretion, may consider a solution that does include all or any of these deliverables or consider deliverables not originally listed. An offeror **must** highlight any deliverable it does not meet and give any suggested “work-around” or future date that it **will** be able to provide the deliverable.

6 FORMAT OF SUBMISSION

All proposals should be prepared simply and economically and provide a direct, concise explanation of the offeror’s proposal and qualifications. Elaborate brochures, sales literature and other presentations unnecessary to a complete and effective proposal are not desired.

Offerors are required to provide an electronic copy of their response. The electronic copy should be provided in MS WORD or in PDF format, except for the project plan, which can be in MS Project. The submission must be delivered as indicated in Section 1.6 of this document. An Original and three (3) copies shall be submitted along with the electronic copy.

The offeror is cautioned that it is the offeror's sole responsibility to submit information related to the evaluation categories and that the State of South Dakota is under no obligation to solicit such information if it is not included with the proposal. The offeror's failure to submit such information may cause an adverse impact on the evaluation of the proposal. The offeror should respond to each point in the Scope of Work and Deliverables in the order they were presented.

Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all questions or comments regarding the RFP or the evaluation to the buyer of record indicated on the first page of this RFP. Offerors and their agents may not contact any state employee other than the buyer of record regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should email the buyer of record at Cole.Pry@state.sd.us.

The offeror may be required to submit a copy of its most recent audited financial statements upon the State’s request.

The proposal should be page numbered and should have an index or a table of contents referencing the appropriate page number. Each of the sections listed below should be tabbed.

Offerors are cautioned that use of the State Seal in any of their documents is illegal as per South Dakota Codified Law § 1-6-3.1. *Use of seal or facsimile without authorization prohibited--Violation as misdemeanor. No person may reproduce, duplicate, or otherwise use the official seal of the State of South Dakota, or its facsimile, adopted and described in §§ 1-6-1 and 1-6-2 for any for-profit, commercial purpose without specific authorization from the secretary of state. A violation of this section is a Class 1 misdemeanor.*

Proposals should be prepared using the following headings and, in the order that they are presented below. Please reference the section for details on what should be included in your proposal.

- Executive Summary – This should briefly describe the vendors proposal and must indicate any requirements that cannot be met by the vendor. Proprietary information request should be identified in this section.
- Statement of Understanding of Project
- Deliverables/ Project Plan/Roadmap – A complete narrative of the vendor's assessment of the work to be performed, the vendor's ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the vendor's understanding of the desired overall performance expectations. A specific point-by-point response, in the order listed to each requirement in the RFP. The response should identify each requirement being addressed as enumerated in the RFP. A clear description of any options or alternatives proposed.
- Assessment for Business Optimization (if not included above)
- Gap Analysis (if not included already)
- Non-standard Software and/or Hardware
- System Diagram (If not a separate document)
- Security and Vendor Questions (If not a separate document
- Response to the State's contract terms
- Corporate Qualification
- Project Experience
- Team Organization
- Staffing (FTE)
- Costs (If not a separate document)
- The State of South Dakota's Request for Proposal from completed and Signed

6.1 STATEMENT OF UNDERSTANDING OF PROJECT

To demonstrate your comprehension of the project, the offeror should summarize their understanding of what the work is and what the work will entail. This should include, but not be limited to, the offeror's understanding of the purpose and scope of the project, critical success factors and potential problems related to the project, and the offeror's understanding of the deliverables. The offeror should include their specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements. This section should be limited to no more than two pages.

6.2 CORPORATE QUALIFICATIONS

Please provide responses to the each of the following questions in your proposal.

A. What year was your parent company (if applicable) established?

B. What is the business of your parent company?

C. What is the total number of employees in the parent company?

D. What are the total revenues of your parent company?

E. How many employees of your parent company have the skill set to support this effort?

F. How many of those employees are accessible to your organization for <u>active</u> support?

G. What year was your firm established?

H. Has your firm ever done business under a different name and if so, what was the name?

I. How many employees does your firm have?

J. How many employees in your firm are involved in this type of project?

K. How many of those employees are involved in on-site project work?

L. What percent of your parent company's revenue (if applicable), is produced by your firm?

M. Corporate resources available to perform the work, including any specialized services, within the specified time limits for the project

N. Availability to the project locale

O. Familiarity with the project locale

P. Has your firm ever done business with other governmental agencies? If so, please provide references.

Q. Has your firm ever done business with the State of South Dakota? If so, please provide references.

R. Has your firm ever done projects that are like or similar to this project? If so, how many clients are using your solution? Please provide a list of four or more locations of the same approximant nature as the State where your application is in use along with contact names and numbers for those sites. The State of South Dakota has a consolidated IT system. **Either** any references given should be from states with a consolidated IT system, to be acceptable **or** the reference should be a detailed explanation on how you will modify your work plan for a consolidated environment that you are unfamiliar with.

S. Provide the reports of third-party security scans done at the end of the four projects you provided in your proposal response. If there are no audits of these projects then provide, unedited and un-redacted results of such security testing/scanning from third-party companies or tools that has been run within the past 90 days. The State will sign a non-disclosure agreement, as needed, and redaction of these scan reports can be done within the limits of the State's open records law.

T. What is your Company's web site?

When providing references, the reference must include the following information:

- Name, address and telephone number of client/contracting agency and a representative of that agency who may be contacted for verification of all information submitted
- Dates of the service/contract
- A brief, written description of the specific prior services performed and requirements thereof

6.3 RELEVANT PROJECT EXPERIENCE

Provide details about four recent projects that the offeror was awarded and then managed through to completion. Project examples should include sufficient detail so the agency fully understands the goal of the project; the dates (from start to finish) of the project; the offeror's scope of work for the project; the responsibilities of the offeror and subcontractors in the project; the complexity of the offeror's involvement in the project; deliverables provided by the offeror; the methodologies employed by the offeror; level and type of project management responsibilities of the offeror; changes that were made and request for changes that differed from the onset of the project; how changes to the project goals, offeror's scope of work, and deliverables were addressed or completed; price and cost data; quality of the work and the total of what the offeror accomplished in the project.

A. Client/Company Name

B. Client Company Address, including City, State and Zip Code

C. Client/Company Contacts(s)
Name
Title
Telephone Number
E-mail address
Fax Number

D. Project Start Date

E. Project Completion Date

F. Project Description and Goals

G. Offeror's Role in Project

H. Offeror's responsibilities

I. Offeror's Accomplishments

J. Description of How Project Was Managed

K. Description of Price and Cost Data from Project

L. Description of special project constraints, if applicable

M. Description of your ability and proven history in handling special project constraints

N. Description of All Changes to the Original Plan or Contract That Were Requested

O. Description of All Changes to the Original Plan or Contract That Offeror Completed

P. Description of How Change Requests Were Addressed or Completed by Offeror

Q. Was Project Completed in a Timeframe That Was According to the Original Plan or Contact? (If "No", provide explanation)

R. Was Project Completed Within Original Proposed Budget? (If "No" provide explanation)

S. Was there any Litigation or Adverse Contract Action regarding Contract Performance? (If "Yes" provide explanation)

T. Feedback on Offeror's Work by Company/Client

U. Offeror's Statement of Permission for the Department to Contact the Client/Company and for the Client's/Company's Contract(s) to Release Information to the Department

6.4 PROJECT PLAN

Provide a project plan that indicates how you will complete the required deliverables and services and addresses the following:

- Proposed project management techniques
- Number of offeror's staff needed
- Tasks to be performed (within phase as applicable)
- Number of hours each task will require
- Deliverables created by each task
- Dates by which each task will be completed (dates should be indicated in terms of elapsed time from project inception)
- Resources assigned to each task
- Required state agency support
- Show task dependencies
- Training

Microsoft Project is the standard scheduling tool for the State of South Dakota. The schedule should be a separate document, provided in Microsoft Excel, and submitted as an attachment to your proposal.

If, as part of this project, the offeror plans to set up or configure the software or hardware and plans to do this outside of South Dakota, even in part, then the offeror needs to provide a complete and detailed project plan on how the offeror plans on migrating to the State's site. Failure to do this is sufficient grounds to disregard the submission, as it demonstrates that the offeror fundamentally does not understand the project. Providing a work plan for the steps above that is complete and detailed maybe sufficient.

6.5 DELIVERABLES

This section should constitute the major portion of the work to be performed. Provide a complete narrative detailing the assessment of the work to be performed, approach and methods to provide the requirements of this RFP, the offeror's ability to fulfill the requirements of this RFP, the offeror's approach, the resources necessary to fulfill the requirements, project management techniques, specialized services, availability to the project locale, familiarity with the project locale and a description of any options or alternatives proposed. This should demonstrate that the offeror understands the desired overall performance expectations. This response should identify each requirement being addressed as enumerated in section 8. If you have an alternative methodology or deliverables you would like to propose, please include a detailed description of the alternative methodology or deliverables and how they will meet or exceed the essential requirements of the methodology and deliverables described in Section 6.

6.6 NON-STANDARD HARDWARE AND SOFTWARE

State standard hardware and software should be utilized unless there is a reason not to. If your proposal will use non-standard hardware or software, you must first obtain State approval. If your proposal recommends using non-standard hardware or software, the proposal should very clearly indicate what non-standard hardware or software is being proposed and why it is necessary to use non-standard hardware or software to complete the project requirements. The use of non-standard hardware or software requires use of the State's New Product Process. This process can be found through the Standards' page and must be performed by State employees. The costs of such non-standard hardware or software should be reflected in your cost proposal. The work plan should also account for the time needed to complete the New Product Process. See https://bit.sd.gov/bit?id=bit_standards_overview, for lists of the State's standards. The proposal should also include a link to your hardware and software specifications.

If non-standard hardware or software is used, the project plan and the costs stated in Section 7 must include service desk and field support, since BIT can only guarantee best effort support for standard hardware and software. If any software development may be required in the future, hourly development rates must be stated. The project plan must include the development and implementation of a disaster recovery plan since non-standard hardware and software will not be covered by the State's disaster recovery plan. This must also be reflected in the costs.

The offeror must complete the list of technical questions, Security and Vendor Questions which is attached as Appendix B. These questions and the offeror's responses may be used in the proposal evaluation.

6.7 Background Checks

The offeror must include the following statement in its proposal:

(Company name here) acknowledges and affirms that it understands that the (company name here) employees who have access to production Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), any information defined under state statute as confidential or have access to secure facilities will have fingerprint-based background checks. These background checks will be used to check the criminal history records of the State as well as the Federal Bureau of Investigation's records. (Company name here) acknowledges and affirms that this requirement will extend to include any Subcontractor's, Agents, Assigns and or Affiliated Entities employees.

7 COST PROPOSAL

All costs related to the provision of the required services must be included in each cost proposal offered.

The offeror must submit a statement in the Proposal that attests the offeror's willingness and ability to perform the work described in this RFP for the price being offered.

7.1 STAFFING (FTE)

Below is and example of the table that can be used for the staffing (FTE) matrix requested.

Name	Role	Total Hours on Project	Total Hours on Site	Hourly Rate	Total
				Total:	

7.2 ADDITIONAL WORK

The offeror may be expected to perform additional work as required by any of the State signatories to a contract. This work can be made a requirement by the State for allowing the application to go into production. This additional work will not be considered a project change chargeable to the State if it is for reasons of correcting security deficiencies, meeting the functional requirements established for the application, unsupported third-party technologies or excessive resource consumption. The cost for additional work should be included in your proposal.

8 PROPOSAL EVALUATION AND AWARD PROCESS

8.1 After determining that a proposal satisfies the mandatory requirements stated in the Request for Proposal, the evaluator(s) shall use subjective judgment in conducting a comparative assessment of the proposal by considering each of the following criteria:

8.1.1 Capability, Capacity & Qualification

Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration;

8.1.2 Staffing Plan and Staff Qualifications

Resources available to perform the work, including any specialized services, within the specified time limits for the project;

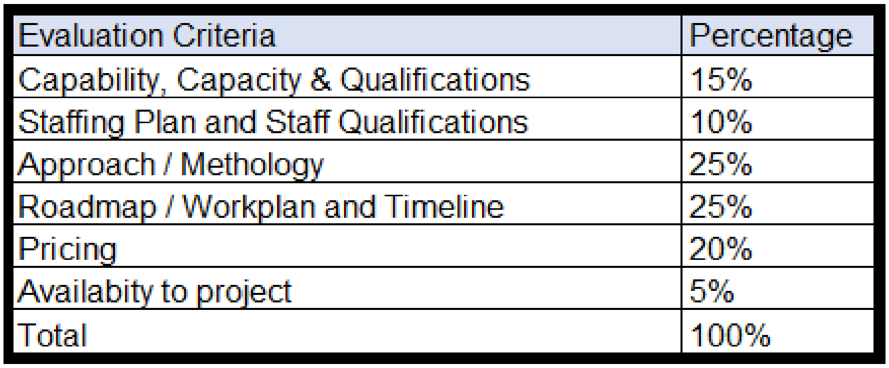
8.1.3 Approach and Methodology
Specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements; administration;

8.1.4 Roadmap/Workplan and Timeline
Proposed project management techniques including a roadmap, workplan and timeline of deliverables, this should include an ability and proven history in handling special project constraints and the plan to overcome constraints;

8.1.5 Pricing
Proposed pricing; and

8.1.6 Availability to project
Availability to the project locale and familiarity with the project locale

Below is the scoring criteria that will be used broke out by percentage system



Evaluation Criteria	Percentage
Capability, Capacity & Qualifications	15%
Staffing Plan and Staff Qualifications	10%
Approach / Methology	25%
Roadmap / Workplan and Timeline	25%
Pricing	20%
Availabity to project	5%
Total	100%

8.2 Experience and reliability of the offeror's organization are considered subjectively in the evaluation process. Therefore, the offeror is advised to submit any information which documents successful and reliable experience in past performances, especially those performances related to the requirements of this RFP.

8.3 The qualifications of the personnel proposed by the offeror to perform the requirements of this RFP, whether from the offeror's organization or from a proposed subcontractor, will be subjectively evaluated. Therefore, the offeror should submit detailed information related to the experience and qualifications, including education and training, of proposed personnel.

8.4 The State reserves the right to reject any or all proposals, waive technicalities, and make award(s) as deemed to be in the best interest of the State of South Dakota.

8.5 Award

The requesting agency and the highest ranked offeror shall mutually discuss and refine the scope of services for the project and shall negotiate terms, including compensation and performance schedule.

8.5.1 If the agency and the highest ranked offeror are unable for any reason to negotiate a contract at a compensation level that is reasonable and fair to the agency, the agency shall, either orally or in writing, terminate negotiations with the offeror. The agency may then negotiate with the next highest ranked offeror.

8.5.2 The negotiation process may continue through successive offerors, according to agency ranking, until an agreement is reached, or the agency terminates the contracting process.

9 BEST AND FINAL OFFERS

The State reserves the right to request best and final offers. If so, the State will initiate the request for best and final offers; best and final offers may not be initiated by an offeror. Best and final offers may not be necessary if the State is satisfied with the proposals received.

If best and final offers are sought, the State will document which offerors will be notified and provide them opportunity to submit best and final offers. Requests for best and final offers will be sent stating any specific areas to be covered and the date and time in which the best and final offer must be returned. Conditions, terms, or price of the proposal may be altered or otherwise changed, provided the changes are within the scope of the request for proposals and instructions contained in the request for best and final offer. If an offeror does not submit a best and final offer or a notice of withdrawal, the offeror's previous proposal will be considered that offeror's best and final proposal. After best and final offers are received, final evaluations will be conducted.

10 SCANNING

The offeror acknowledges that the State will conduct a security and vulnerability scan as part of the review of the offeror’s RFP. This scan will not include a penetration test. The State will use commercially available, industry standard tools to scan a non-production environment with non-production data at mutually agreeable times.

The offeror should fill in the information below and sign the form. The offeror’s employee signing this form must have the authority to allow the State to do a security scan. If no security contact is given the State will assume that the State can scan at any time. **At the state’s option, any RFP response that does not include a completed and signed form may be dropped from consideration. If there is State data protected by federal or state law or regulation or industry standard involved, the State is more likely to consider a security scan necessary for an RFP to be considered.** Except for State staff, the State will only provide scan information to the offeror’s security contact. At the State’s option, the State will conduct the scan at a location named by the offeror. The offeror can only request, not require, naming the scanning location. The State may consider a comprehensive, complete and recent risk assessment as satisfying the scanning requirement. If required, the State will sign a non-disclosure agreement before scanning or receiving the risk assessment.

Offeror’s name: ________________________

Offeror’s security contact’s name: ________________________

Security contact’s phone number: ________________________

Security contact’s email address: ________________________

Web address URL or Product Name _____________________. The State will contact the security contact to arrange for a test log for scanning.

Offeror’s employee acknowledging the right to scan:

Name (Print): ______________________

Title: _______________________________

Date: _______________________________

Signature: ___________________________

Exhibit A
Bureau of Information and Telecommunications
Required IT Contract Terms

Any contract resulting from this RFP will include the State's required IT terms and conditions as listed below, along with any additional terms and conditions as negotiated by the parties. Due to the changing landscape of IT security and data privacy, the State reserves the right to add additional IT terms and conditions or modify the IT terms and conditions listed below to the resulting contract:

Pursuant to South Dakota Codified Law § 1-33-44, the Bureau of Information and Telecommunications ("BIT") oversees the acquisition of office systems technology, software, and services; telecommunication equipment, software, and services; and data processing equipment, software, and services for departments, agencies, commissions, institutions, and other units of state government. As part of its duties as the Executive Branch's centralized IT agency, BIT requires the contract terms and conditions of this Exhibit XX. For purposes of this Exhibit, [Vendor Name] will be referred to as the "Vendor."
It is understood and agreed to by all parties that BIT has reviewed and approved only this Exhibit. Due to the ever-changing security and regulatory landscape in IT and data privacy, before renewal of this Agreement BIT must review and approve the clauses found in this Exhibit as being the then current version of the clauses and if any additional required clauses are needed. Changes to clauses in this Exhibit must be approved in writing by all parties before they go into effect and a renewal of this Agreement is possible.

The Parties agree, when used in this Exhibit, the term "Vendor" will mean the Vendor and the Vendor's employees, subcontractors, agents, assigns, and affiliated entities.

Section I. Confidentiality of Information

For purposes of this paragraph, "State Proprietary Information" will include all information disclosed to the Vendor by the State. The Vendor will not disclose any State Proprietary Information to any third person for any reason without the express written permission of a State officer or employee with authority to authorize the disclosure. The Vendor must not: (i) disclose any State Proprietary Information to any third person unless otherwise specifically allowed under this Agreement; (ii) make any use of State Proprietary Information except to exercise rights and perform obligations under this Agreement; (iii) make State Proprietary Information available to any of its employees, officers, agents, or third party consultants except those who have a need to access such information and who have agreed to obligations of confidentiality at least as strict as those set out in this Agreement. The Vendor is held to the same standard of care in guarding State Proprietary Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding State Proprietary Information in the strictest confidence. The Vendor must protect the confidentiality of the State's information from the time of receipt to the time that such information is either returned to the State or destroyed to the extent that it cannot be recalled or reproduced. The Vendor agrees to return all information received from the State to the State's custody upon the end of the term of this Agreement, unless otherwise agreed in a writing signed by both parties. State Proprietary Information will not include information that:

A. was in the public domain at the time it was disclosed to the Vendor,

B. was known to the Vendor without restriction at the time of disclosure from the State,
C. that was disclosed with the prior written approval of State's officers or employees having authority to disclose such information,
D. was independently developed by the Vendor without the benefit or influence of the State's information, and
E. becomes known to the Vendor without restriction from a source not connected to the State of South Dakota.

State's Proprietary Information can include names, social security numbers, employer numbers, addresses and other data about applicants, employers or other clients to whom the State provides services of any kind. The Vendor understands that this information is confidential and protected under State law. The Parties mutually agree that neither of them nor any subcontractors, agents, assigns, or affiliated entities will disclose the contents of this Agreement except as required by applicable law or as necessary to carry out the terms of the Agreement or to enforce that Party's rights under this Agreement. The Vendor acknowledges that the State and its agencies are public entities and thus may be bound by South Dakota open meetings and open records laws. It is therefore not a breach of this Agreement for the State to take any action that the State reasonably believes is necessary to comply with South Dakota open records or open meetings laws.

Section II. Cyber Liability Insurance

The Vendor will maintain cyber liability insurance with liability limits in the amount of $_________ to protect any and all State Data the Vendor receives as part of the project covered by this agreement including State Data that may reside on devices, including laptops and smart phones, utilized by Vendor employees, whether the device is owned by the employee or the Vendor. If the Vendor has a contract with a third-party to host any State Data the Vendor receives as part of the project under this Agreement, then the Vendor will include a requirement for cyber liability insurance as part of the contract between the Vendor and the third-party hosting the data in question. The third-party cyber liability insurance coverage will include State Data that resides on devices, including laptops and smart phones, utilized by third-party employees, whether the device is owned by the employee or the third-party Vendor. The cyber liability insurance will cover expenses related to the management of a data breach incident, the investigation, recovery and restoration of lost data, data subject notification, call management, credit checking for data subjects, legal costs, and regulatory fines. Before beginning work under this Agreement, the Vendor will furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement and which provide that such insurance may not be canceled, except on 30 days prior written notice to the State. The Vendor will furnish copies of insurance policies if requested by the State. The insurance will stay in effect for three years after the work covered by this Agreement is completed.

Section III. Rejection or Ejection of Vendor

The State, at its option, may require the vetting of any of the Vendor, and the Vendor's subcontractors, agents, Assigns, or affiliated entities. The Vendor is required to assist in this process as needed.

The State reserves the right to reject any person from participating in the project or require the Vendor to remove from the project any person the State believes is detrimental to the project or is considered by the State to be a security risk. The State will provide the Vendor with notice of its determination, and the reasons for the rejection or removal if requested by the Vendor. If the State signifies that a potential security violation exists with respect to the request, the Vendor must immediately remove the individual from the project.

Section IV. Software Functionality and Replacement

The software licensed by the Vendor to the State under this Agreement will provide the functionality as described in the software documentation, which the Vendor agrees to provide to the State prior to or upon the execution of this Agreement.
The Vendor agrees that:

A. If, in the opinion of the State, the Vendor reduces or replaces the functionality contained in the licensed product and provides this functionality as a separate or renamed product, the State will be entitled to license such software product at no additional license or maintenance fee.
B. If, in the opinion of the State, the Vendor releases an option, future product, purchasable product or other release that has substantially the same functionality as the software product licensed to the State, and it ceases to provide maintenance for the older software product, the State will have the option to exchange licenses for such replacement product or function at no additional charge. This includes situations where the Vendor discontinues the licensed product and recommends movement to a new product as a replacement option regardless of any additional functionality the replacement product may have over the licensed product.

Section V. Federal Intellectual Property Bankruptcy Protection Act

The Parties agree that the State will be entitled to all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto. The State also maintains its termination privileges if the Vendor enters bankruptcy.

Section VI. Non-Disclosure and Separation of Duties

The Vendor will enforce separation of job duties and require non-disclosure agreements of all staff that have or can have access to State Data or the hardware that State Data resides on. The Vendor will limit staff knowledge to those staff who duties that require them to have access to the State Data or the hardware the State Data resides on.

Section VII. Cessation of Business

The Vendor will notify the State of impending cessation of its business or that of a tiered provider and the Vendor’s contingency plan. This plan should include the immediate transfer of any previously escrowed assets and data and State access to the Vendor’s facilities to remove or destroy any state-owned assets and data. The Vendor will implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the State. The Vendor will provide a fully documented service description and perform and document a gap analysis by examining any differences between its services and those to be provided by its successor. The Vendor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the State. The Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and impact on the State, all such work to be coordinated and performed in advance of the formal, final transition date.

Section VIII. Legal Requests for Data

Except as otherwise expressly prohibited by law, the Vendor will:

A. Immediately notify the State of any subpoenas, warrants, or other legal orders, demands or requests received by the Vendor seeking State Data maintained by the Vendor,
B. Consult with the State regarding the Vendor's response,
C. Cooperate with the State's requests in connection with efforts by the State to intervene and quash or modify the legal order, demand or request, and
D. Upon the State's request, provide the State with a copy of both the demand or request and its proposed or actual response.

Section IX. eDiscovery

The Vendor will contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to State Data. The Vendor will not respond to service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

Section X. Audit Requirements

The Vendor warrants and agrees it is aware of and complies with all audit requirements relating to the classification of State Data the Vendor stores, processes, and accesses. Depending on the data classification, this may require the Vendor to grant physical access to the data hosting facilities to the State or a federal agency. The Vendor will notify the State of any request for physical access to a facility that hosts or processes State Data by any entity other than the State.

Section XI. Annual Risk Assessment

The Vendor will conduct an annual risk assessment or when there has been a significant system change. The Vendor will provide verification to the State's contact upon request that the risk assessment as taken place. At a minimum, the risk assessment will include a review of the:

A. Penetration testing of the Vendor's system;
B. Security policies and procedures;
C. Disaster recovery plan;
D. Business Associate Agreements; and
E. Inventory of physical systems, devices, and media that store or utilize ePHI for completeness.

If the risk assessment provides evidence of deficiencies, a risk management plan will be produced. Upon request by the State, the Vendor will send a summary of the risk management plan to the State's contact. The summary will include completion dates for the risk management plan's milestones. Upon request by the State, the Vendor will send updates on the risk management plan to the State's contact. Compliance with this Section may be met if the Vendor provides proof to the State that the Vendor is FedRAMP Certified and has maintained FedRAMP Certification.

Section XII. Independent Audit

The Vendor will disclose any independent audits that are performed on any of the Vendor's systems tied to storing, accessing, and processing State Data. This information on an independent audit(s) must be provided to the State in any event, whether the audit or certification process is successfully completed or not. The Vendor will provide a copy of the findings of the audit(s) to the State. Compliance with this Section may be met if the Vendor provides a copy of the Vendor's SOC 2 Type II report to the State upon request.

Section XIII. Service Level Agreements

The Vendor warrants and agrees that the Vendor has provided to the State all Service Level Agreements (SLA) related to the deliverables of the Agreement. The Vendor further warrants that it will provide the deliverables to the State in compliance with the SLAs.

Section XIV. Access Attempts

The Vendor will log all access attempts, whether failed or successful, to any system connected to the hosted system which can access, read, alter, intercept, or otherwise impact the hosted system or its data or data integrity. For all systems, the log must include at least: login page used, username used, time and date stamp, incoming IP for each authentication attempt, and the authentication status, whether successful or not. Logs must be maintained not less than 7 years in a searchable database in an electronic format that is un-modifiable. At the request of the State, the Vendor agrees to grant the State access to those logs to demonstrate compliance with the terms of this Agreement and all audit requirements related to the hosted system.

Section XV. Access to State Data

Unless this Agreement is terminated, the State's access to State Data amassed pursuant to this Agreement will not be hindered if there is a:

A. Contract dispute between the parties to this Agreement,
B. There is a billing dispute between the parties to this Agreement, or
C. The Vendor merges with or is acquired by another company.

Section XVI. Password Protection

All aspects of the Vendor's products provided to the State pursuant to this Agreement will be password protected. If the Vendor provides the user with a preset or default password, that password cannot include any Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), or any information defined under federal or state law, rules, or regulations as confidential information or fragment thereof. On an annual basis, the Vendor will document its password policies for all Vendor employees to ensure adequate password protections are in place. The process used to reset a password must include security questions or Multifactor Authentication. Upon request, the Vendor will provide to the State the Vendor's password policies, logs, or administrative settings to demonstrate the password policies are actively enforced.

Section XVII. Provision of Data

State Data is any data produced or provided by the State as well as any data produced or provided for the State by the Vendor or a third-party.

Upon notice of termination by either party or upon reaching the end of the term of this Agreement, the Vendor will provide the State all current State Data in a non-proprietary format. In addition, the Vendor agrees to extract any information (such as metadata, which includes data structure descriptions, data dictionary, and data) stored in repositories not hosted on the State's IT infrastructure in a format chosen by the State. If the State's chosen format is not possible, the Vendor will extract the information into a text file format and provide it to the State.

Upon the effective date of the termination of this Agreement, the Vendor will again provide the State with all current State Data in a non-proprietary format. In addition, the Vendor will again extract any information (such as metadata) stored in repositories not hosted on the State's IT infrastructure in a format chosen by the State. As before, if the State's chosen format is not possible, the Vendor will extract the information into a text file format and provide it to the State.

Section XVIII. Threat Notification

A credible security threat consists of the discovery of an exploit that a person considered an expert on Information Technology security believes could be used to breach any aspect of a system that is holding State Data or a product provided by the Vendor. Upon becoming aware of a credible security threat with the Vendor's product(s) and or service(s) being used by the State, the Vendor or any subcontractor supplying product(s) or service(s) to the Vendor needed to fulfill the terms of this Agreement will notify the State within two business days of any such threat. If the State requests, the Vendor will provide the State with information on the threat.

Section XIX. Security Incident Notification for Non-Health Information

The Vendor will implement, maintain, and update Security Incident procedures that comply with all State standards and Federal and State requirements. A Security Incident is a violation of any BIT security or privacy policies or contract agreements involving sensitive information, or the imminent threat of a violation. The BIT security policies can be found in the Information Technology Security Policy ("ITSP") attached as Exhibit __________. The State requires notification of a Security Incident involving any of the State's sensitive data in the Vendor's possession. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute Security Incidents, this Agreement constitutes notice by the Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State will be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Vendor's firewall, port scans, and unsuccessful log-on attempts, if such probes and reconnaissance scans do not result in a Security Incident as defined above. Except as required by other legal requirements the Vendor will only provide notice of the incident to the State. The State will determine if notification to the public will be by the State or by the Vendor. The method and content of the notification of the affected parties will be coordinated with, and is subject to approval by the State, unless required otherwise by legal requirements. If the State decides that the Vendor will be distributing, broadcasting to or otherwise releasing information on the Security Incident to the news media, the State will decide to whom the information will be sent, and the State must approve the content of any information on the Security Incident before it may be distributed, broadcast, or otherwise released. The Vendor must reimburse the State for any costs associated with the notification, distributing, broadcasting, or otherwise releasing information on the Security Incident.

A. The Vendor must notify the State contact within 12 hours of the Vendor becoming aware that a Security Incident has occurred. If notification of a Security Incident to the State contact is delayed because it may impede a criminal investigation or jeopardize homeland or federal security, notification must be given to the State within 12 hours after law-enforcement provides permission for the release of information on the Security Incident.

B. Notification of a Security Incident at a minimum is to consist of the nature of the data exposed, the time the incident occurred, and a general description of the circumstances of the incident. If all of the information is not available for the notification within the specified time period, the Vendor must provide the State with all of the available information along with the reason for the incomplete notification. A delay in excess of 12 hours is acceptable only if it is necessitated by other legal requirements.

C. At the State's discretion within 12 hours the Vendor must provide to the State all data available including:

1. name of and contact information for the Vendor's Point of Contact for the Security Incident,
2. date and time of the Security Incident,
3. date and time the Security Incident was discovered,
4. description of the Security Incident including the data involved, being as specific as possible,
5. the potential number of records, and if unknown the range of records,
6. address where the Security Incident occurred, and
7. the nature of the technologies involved. If not all of the information is available for the notification within the specified time period, the Vendor must provide the State with all of the available information along with the reason for the incomplete information. A delay in excess of 12 hours is acceptable only if it is necessitated by other legal requirements.

D. If the Security Incident falls within the scope of South Dakota Codified Law Chapter 22-40, the Vendor is required to comply with South Dakota law.

The requirements of subsection D of this Section do not replace the requirements of subsections A, B, and C, but are in addition to them.

Section XX. Handling of Security Incident for Non-Health Information

At the State's discretion, the Vendor will preserve all evidence regarding a security incident including but not limited to communications, documents, and logs. The Vendor will also:

A. fully investigate the incident,
B. cooperate fully with the State's investigation of, analysis of, and response to the incident,
C. make a best effort to implement necessary remedial measures as soon as it is possible, and
D. document responsive actions taken related to the Security Incident, including any post-incident review of events and actions taken to implement changes in business practices in providing the services covered by this Agreement.

If, at the State's discretion the Security Incident was due to the actions or inactions of the Vendor and at the Vendor's expense the Vendor will use a credit monitoring service, call center, forensics company, advisors, or public relations firm whose services are acceptable to the State. At the State's discretion the Vendor will offer two years of credit monitoring to each person whose data was compromised. The State will set the scope of any investigation. The State reserves the right to require the Vendor undergo a risk assessment where the State will determine the methodology and scope of the assessment and who will perform the assessment (a third-party vendor may be used). Any risk assessment required by this Section will be at the Vendor's expense.

If the Vendor is required by federal law or regulation to conduct a Security Incident or data breach investigation, the results of the investigation must be reported to the State within 12 hours of the investigation report being completed. If the Vendor is required by federal law or regulation to notify the affected parties, the State must also be notified, unless otherwise required by law.

Notwithstanding any other provision of this Agreement, and in addition to any other remedies available to the State under law or equity, the Vendor will reimburse the State in full for all costs incurred by the State in investigation and remediation of the Security Incident including, but not limited, to providing notification to regulatory agencies or other entities as required by law or contract. The Vendor will also pay all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident.

Section XXI. Adverse Event

The Vendor must notify the State contact within three days if the Vendor becomes aware that an Adverse Event has occurred. An Adverse Event is the unauthorized use of system privileges, unauthorized access to State Data, execution of malware, physical intrusions and electronic intrusions that may include network, applications, servers, workstations, and social engineering of staff. If the Adverse Event was the result of the Vendor's actions or inactions, the State can require a risk assessment of the Vendor the State mandating the methodology to be used as well as the scope. At the State's discretion a risk assessment may be performed by a third party at the Vendor's expense. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party.

Section XXII. Browser

The system, site, or application must be compatible with Vendor supported versions of Edge, Chrome, Safari, and Firefox browsers. Silverlight, QuickTime, PHP, Adobe ColdFusion, and Adobe Flash will not be used in the system, site, or application. Adobe Animate CC is allowed if files that require third-party plugins are not required.

Section XXIII. Security Acknowledgment Form

The Vendor will be required to sign the Security Acknowledgement Form which is attached to this Agreement as Exhibit ________________________. The signed Security Acknowledgement Form must be submitted to the State and approved by the South Dakota Bureau of Information and Telecommunications and communicated to the Vendor by the State contact before work on the contract may begin. This Security Acknowledgment Form constitutes the agreement of the Vendor to be responsible and liable for ensuring that the Vendor, the Vendor's employee(s), and subcontractor's, agents, assigns and affiliated entities and all of their employee(s), participating in the work will abide by the terms of the Information Technology Security Policy (ITSP) attached to this Agreement. Failure to abide by the requirements of the ITSP or the Security Acknowledgement Form can be considered a breach of this Agreement at the discretion of the State. It is also a breach of this Agreement, at the discretion of the State, if the Vendor does not sign another Security Acknowledgement Form covering any employee(s) and any subcontractor's, agent's, assign's, or affiliated entities' employee(s), any of whom are participating in the work covered by this Agreement, and who begin working under this Agreement after the project has begun. Any disciplining of the Vendor's, Vendor's employee(s), or subcontractor's, agent's, assign's, or affiliated entities' employee(s) due to a failure to abide by the terms of the Security Acknowledgement Form will be done at the discretion of the Vendor or subcontractors, agents, assigns, or affiliated entities and in accordance with the Vendor's or subcontractor's, agent's, assign's, and affiliated entities' personnel policies. Regardless of the actions taken by the Vendor and subcontractors, agents, assigns, and affiliated entities, the State will retain the right to require at the State's discretion the removal of the employee(s) from the project covered by this Agreement.

Section XXIV. Background Investigations

The State requires any person who writes or modifies State-owned software, alters hardware, configures software of State-owned technology resources, has access to source code or protected Personally Identifiable Information (PII) or other confidential information, or has access to secure areas to undergo fingerprint-based background investigations. These fingerprints will be used to check the criminal history records of both the State of South Dakota and the Federal Bureau of Investigation. These background investigations must be performed by the State with support from the State's law enforcement resources. The State will supply the fingerprint cards and prescribe the procedure to be used to process the fingerprint cards. Project plans should allow 2-4 weeks to complete this process.

If work assignments change after the initiation of the project covered by this Agreement so that a new person will be writing or modifying State-owned software, altering hardware, configuring software of State-owned technology resources, have access to source code or protected PII or other confidential information, or have access to secure areas, background investigations must be performed on the individual who will complete any of the referenced tasks. The State reserves the right to require the Vendor to prohibit any person from performing work under this Agreement whenever the State believes that having the person performing work under this Agreement is detrimental to the project or is considered by the State to be a security risk, based on the results of the background investigation. The State will provide the Vendor with notice of this determination.

Section XXV. Information Technology Standards

Any service, software, or hardware provided under this Agreement will comply with State standards which can be found at https://bit.sd.gov/bit?id=bit_standards_overview.

Section XXVI. Product Usage

The State cannot be held liable for any additional costs or fines for mutually understood product usage over and above what has been agreed to in this Agreement unless there has been an audit conducted on the product usage. This audit must be conducted using a methodology agreed to by the State. The results of the audit must also be agreed to by the State before the State can be held to the results. Under no circumstances will the State be required to pay for the costs of said audit.

Section XXVII. Malicious Code

A. The Vendor warrants that the Agreement deliverables contain no code that does not support an application requirement.
B. The Vendor warrants that the Agreement deliverables contains no malicious code.
C. The Vendor warrants that the Vendor will not insert into the Agreement deliverables or any media on which the Agreement deliverables is delivered any malicious or intentionally destructive code.
D. In the event any malicious code is discovered in the Agreement deliverables, the Vendor must provide the State at no charge with a copy of or access to the applicable Agreement deliverables that contains no malicious code or otherwise correct the affected portion of the services provided to the State. The remedies in this Section are in addition to other additional remedies available to the State.

Section XXVIII. License Agreements

The Vendor warrants that it has provided to the State and incorporated into this Agreement all license agreements, End User License Agreements (EULAs), and terms of use regarding its software or any software incorporated into its software before execution of this Agreement. Failure to provide all such license agreements, EULAs, and terms of use will be a breach of this Agreement at the option of the State. The parties agree that neither the State nor its end users will be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this Agreement. Any changes to the terms of this Agreement or any additions or subtractions must first be agreed to by both parties in writing before they go into effect. This paragraph will control and supersede the language of any such agreements to the contrary.

Section XXIX. Web and Mobile Applications

A. The Vendor's application is required to:

1. have no code or services including web services included in or called by the application unless they provide direct, functional requirements that support the State's business goals for the application,
2. encrypt data in transport and at rest using a mutually agreed upon encryption format,
3. close all connections and close the application at the end of processing,
4. have documentation that is in grammatically complete text for each call and defined variables (i.e., using no abbreviations and using complete sentences) sufficient for a native speaker of English with average programming skills to determine the meaning or intent of what is written without prior knowledge of the application,
5. have no code not required for the functioning of application,
6. have no "back doors", a back door being a means of accessing a computer program that bypasses security mechanisms, or other entries into the application other than those approved by the State,
7. permit no tracking of device user's activities without providing a clear notice to the device user and requiring the device user's active approval before the application captures tracking data,
8. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation,
9. fully disclose in the "About" information that is the listing of version information and legal notices, of the connections made, permission(s) required, and the purpose of those connections and permission(s),
10. ask only for those permissions and access rights on the user's device that are required for the defined requirements of the Vendor's application,
11. access no data outside what is defined in the "About" information for the Vendor's application,
12. conform to Web Content Accessibility Guidelines 2.0,
13. have Single Sign On capabilities with the State's identity provider,
14. any application to be used on a mobile device must be password protected.

B. The Vendor is required to disclose all:

1. functionality,
2. device and functional dependencies, and
3. third party libraries used.

If the application does not adhere to the requirements given above or the Vendor has unacceptable disclosures, at the State's discretion, the Vendor will rectify the issues at no cost to the State.

Section XXX. Data Location and Offshore Services

The Vendor must provide its services to the State as well as storage of State Data solely from data centers located in the continental United States. The Vendor will not provide access to State Data to any entity or person(s) located outside the continental United States that are not named in this Agreement without prior written permission from the State. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States.

Section XXXI. Vendor Training Requirements

The Vendor, Vendor's employee(s), and Vendor's subcontractors, agents, assigns, affiliated entities and their employee(s), must successfully complete, at the time of hire a cyber-security training program. The training must include but is not limited to:

A. legal requirements for handling data,
B. media sanitation,
C. strong password protection,
D. social engineering, or the psychological manipulation of persons into performing actions that are inconsistent with security practices or that cause the divulging of confidential information, and
E. security incident response.

Section XXXII. Data Sanitization

At the end of the project covered by this Agreement the Vendor, and Vendor's subcontractors, agents, assigns, and affiliated entities will return the State Data or securely dispose of all State Data in all forms, this can include State Data on media such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. This State Data must be permanently deleted by either purging the data or destroying the medium on which the State Data is found according to the methods given in the most current version of NIST 800-88. Certificates of Sanitization for Offsite Data (See bit.sd.gov/vendor/default.aspx for copy of certificate) must be completed by the Vendor and given to the State contact. The State will review the completed Certificates of Sanitization for Offsite Data. If the State is not satisfied by the data sanitization then the Vendor will use a process and procedure that does satisfy the State.

This contract clause remains in effect for as long as the Vendor, and Vendor's subcontractors, agents, assigns, and affiliated entities have the State Data, even after the Agreement is terminated or the project is completed.

Section XXXIII. Use of Portable Devices

The Vendor must prohibit its employees, agents, affiliates, and subcontractors from storing State Data on portable devices, including personal computers, except for devices that are used and kept only at the Vendor's data center(s). All portable devices used for storing State Data must be password protected and encrypted.

Section XXXIV. Remote Access

The Vendor will prohibit its employees, agents, affiliates, and subcontractors from accessing State Data remotely except as necessary to provide the services under this Agreement and consistent with all contractual and legal requirements. The accounts used for remote access cannot be shared accounts and must include multifactor authentication. If the State Data that is being remotely accessed is legally protected data or considered sensitive by the State, then:

A. The device used must be password protected,
B. The data is not put onto mobile media (such as flash drives),
C. No non-electronic copies are made of the data, and
D. A log must be maintained by the Vendor detailing the data which was accessed, when it was accessed, and by whom it was accessed.

The Vendor must follow the State's data sanitization standards, as outlined in this Agreement's Data Sanitization clause, when the remotely accessed data is no longer needed on the device used to access the data.

Section XXXV. Data Encryption

If State Data will be remotely accessed or stored outside the State's IT infrastructure, the Vendor warrants that the data will be encrypted in transit (including via any web interface) and at rest at no less than AES256 level of encryption with at least SHA256 hashing.

Section XXXVI. Rights, Use, and License of and to State Data

The parties agree that all rights, including all intellectual property rights, in and to State Data will remain the exclusive property of the State. The State grants the Vendor a limited, nonexclusive license to use the State Data solely for the purpose of performing its obligations under this Agreement. This Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

Protection of personal privacy and State Data must be an integral part of the business activities of the Vendor to ensure there is no inappropriate or unauthorized use of State Data at any time. To this end, the Vendor must safeguard the confidentiality, integrity, and availability of State Data and comply with the following conditions:

A. The Vendor will implement and maintain appropriate administrative, technical, and organizational security measures to safeguard against unauthorized access, disclosure, use, or theft of Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), or any information that is confidential under applicable federal, state, or international law, rule, regulation, or ordinance. Such security measures will be in accordance with recognized industry practice and not less protective than the measures the Vendor applies to its own non-public data.
B. The Vendor will not copy, disclose, retain, or use State Data for any purpose other than to fulfill its obligations under this Agreement.
C. The Vendor will not use State Data for the Vendor's own benefit and will not engage in data mining of State Data or communications, whether through automated or manual means, except as specifically and expressly required by law or authorized in writing by the State through a State employee or officer specifically authorized to grant such use of State Data.

Section XXXVII. Third Party Hosting

If the Vendor has the State's data hosted by another party, the Vendor must provide the State the name of this party. The Vendor must provide the State with contact information for this third party and the location of their data center(s). The Vendor must receive from the third party written assurances that the State's data will always reside in the continental United States and provide these written assurances to the State. This restriction includes the data being viewed or accessed by the third-party's employees or contractors. If during the term of this Agreement the Vendor changes from the Vendor hosting the data to a third-party hosting the data or changes third-party hosting provider, the Vendor will provide the State with 180 days' advance notice of this change and at that time provide the State with the information required above.

Section XXXVIII. Securing of Data

All facilities used to store and process State Data will employ industry best practices, including appropriate administrative, physical, and technical safeguards to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Vendor's own data of a similar type, and in no event less than commercially reasonable in view of the type and nature of the data involved.

Section XXXIX. Security Processes

The Vendor will disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Vendor. For example: virus checking and port sniffing.

Section XL. Import and Export of Data

The State will have the ability to import or export data piecemeal or in entirety at its discretion without interference from the Vendor. This includes the ability for the State to import or export data to/from other vendors.

Section XLI. Scanning and Audit Authorization

The Vendor will provide the State at no cost and at a date, time, and for duration agreeable to both parties, authorization to scan and access to a test system containing test data for security scanning activities. The system and data provided to the State by the Vendor for testing purposes will be considered a test system containing test data. The State will not scan any environment known by the State to be a production environment at the time the scan is performed by the State. The Vendor provides their consent for the State or any third-party acting for the State to scan the systems and data provided as the State wishes using any methodology that the State wishes. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Vendor or that the Vendor has with a third-party.

The Vendor will also allow the State at the State's expense, not to include the Vendor's expenses, to perform up to two security audit and vulnerability assessments per year to provide verification of the Vendor's IT security safeguards for the system and its data. The State will work with the Vendor to arrange the audit at a time least likely to create workload issues for the Vendor and will accept scanning a test or UAT environment on which the code and systems are a mirror image of the production environment.

Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the State's security scans discover security issues the State may collaborate, at the State's discretion with, the Vendor on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements between the State and the Vendor. In the event of conflicting language, this clause supersedes any other language in this, or any other agreement made between the State and the Vendor.

The Vendor agrees to work with the State to rectify any serious security issues revealed by the security audit or security scanning. This includes additional security audits and security scanning that must be performed after any remediation efforts to confirm the security issues have been resolved and no further security issues exist. If the Vendor and the State agree that scanning results cannot be achieved that are acceptable to the State, then the State may terminate the Agreement without further obligation.

Section XLII. System Upgrades

The Vendor must provide advance notice of 30 days to the State of any major upgrades or system changes the Vendor will be implementing unless the changes are for reasons of security. A major upgrade is a replacement of hardware, software, or firmware with a newer or improved version, in order to bring the system up to date or to improve its characteristics. The State reserves the right to postpone these changes unless the upgrades are for security reasons. The State reserves the right to scan the Vendor's systems for vulnerabilities after a system upgrade. These vulnerability scans can include penetration testing of a test system at the State's discretion.

Section XLIII. Movement of Protected State Data

Any State Data that is protected by federal or state statute or requirements or by industry standards must be kept secure. When protected State Data is moved to any of the Vendor's production or non-production systems, security must be maintained. The Vendor will ensure that that data will at least have the same level of security as it had on the State's environment.

Section XLIV. Banned Services

The Vendor warrants that any hardware or hardware components used to provide the services covered by this Agreement were not manufactured by Huawei Technologies Company or ZTE Corporation, or any subsidiary or affiliate of such entities. Any company considered to be a security risk by the government of the United States under the International Emergency Economic Powers Act or in a United States appropriation bill will be included in this ban.

Section XLV. Multifactor Authentication for Hosted Systems

If the Vendor is hosting on their system or performing Software as a Service where there is the potential for the Vendor or the Vendor's subcontractor to see protected State Data, then Multifactor Authentication (MFA) must be used to before this data can be accessed. The Vendor's MFA, at a minimum must adhere to the requirements of *Level 3 Authentication Assurance for MFA* as defined in NIST 800-63.

Appendix B – Security and Vendor Questions

Agencies: The following questions facilitate agencies acquiring technology that meets state security standards. These questions will assist in improving the quality and the timeliness of the procurement. The Bureau of Information and Telecommunications (BIT) recommends that you utilize your BIT Point of Contact (POC) to set up a planning meeting to review the project and these questions. Understanding the background and context of the questions greatly improves realizing the purpose of the questions. Again, the purpose of the questions is to ensure the product/service being procured will meet the technology and security standards of the state.

If you do not know the details of the technologies the vendor will propose, it is best to keep the question set as broad as possible. If there is a detailed knowledge of what will be proposed, a narrowed set of questions may be possible. Vendors are invited to mark any question that does not apply to their technology as NA (Not Applicable).

Vendors: The following questions help the state determine the best way to assess and integrate your product or service technology with the state's technology infrastructure. Some questions may not apply to the technology you use. In such cases, simply mark the question as NA (Not Applicable). The questions are divided into sections to help identify the point of the questions.

Use the last column as needed to explain your response. Also note, many questions require you to explain your response. The more detailed the response, the better we can understand your product or service.

Where we feel that a Yes/No/NA response is not appropriate, the cell has been grayed out. **If the vendor answers a question by referencing another document or another part of the RFP response, the vendor must provide the page number and paragraph where the information can be found.**

The "BIT" column corresponds to the division within BIT that will be the primary reviewers. If you have questions about the meaning or intent of a question, we can contact the BIT division on your behalf. DC = Data Center; DEV = Development; TEL = Telecommunications; POC = Point of Contract.

<table>
<tr><td colspan="4"><b>System/Product:
The following questions are relevant for all vendors or third parties engaged in this hardware, software, application, or service.</b></td></tr>
<tr><td colspan="4"><b>Response</b></td></tr>
<tr><td><b>#</b></td><td><b>BIT</b></td><td><b>Question</b></td><td><b>Select all that apply</b></td></tr>
<tr><td><b>1</b></td><td>DC
DEV</td><td>Is your proposed solution a cloud-based solution or an on-prem solution?</td><td>☐ State Hosted On-prem (dedicated VM/infrastructure)
☐ State Cloud Provider (PaaS Solution)
☐ Vendor Hosted</td></tr>
<tr><td><b>2</b></td><td>DC
DEV
TEL</td><td>What type of access is required by vendor or proposed solution to state hosted or external resources?</td><td>☐ Not Required
☐ VPN
☐ API
☐ SFTP
☐ Other: (Please state)</td></tr>
<tr><td><b>3</b></td><td>DC</td><td>What type of access is required by vendor to maintain and support the solution?</td><td>☐ Not Required
☐ Citrix (For On-prem)
☐ State Cloud Access
☐ Other: (Please state)</td></tr>
<tr><td><b>4</b></td><td>TEL</td><td>If an on-prem solution, which of the following will apply?</td><td>☐ IoT Hardware
☐ Non-Windows or non-domain joined solution
☐ Windows-based domain joined hardware
☐ Other: (Please state)</td></tr>
</table>

5	DC TEL	Does your proposed solution include/require additional devices connected to the application for activities such as scanning or printing?	☐ Yes ☐ No
6	DC	Does the proposed solution include the use of email?	☐ Yes ☐ No
7	POC TEL	Will there be any desktop software installs, policies, or software required on state managed computers as part of this product?	☐ Yes ☐ No If "Yes", please define:
8	POC	If there are desktop software installs, please provide a link to the licensing requirements or a copy of the licensing requirements.	Please provide link below, if applicable:
9	POC	Will any hardware or peripherals need to be attached to or added to state managed computers?	☐ Yes ☐ No If "Yes", please define:
10	POC	Will any browser plugins be required to install, access, or use this product?	☐ Yes ☐ No If "Yes", please define:
11	POC	Will any products that connect or interact with a state managed computer or network be required as part of this product or project?	☐ Yes ☐ No If "Yes", please define:
12	POC	Will any Bluetooth or RF frequency devices be required as part of this product or project?	☐ Yes ☐ No If "Yes", please define:
13	POC	What operating system is the software/hardware compatible with?	☐ Microsoft Windows 10 ☐ Microsoft Windows 11 ☐ Other (please specify): ☐ N/A

Section A. System Security
The following questions are relevant for all vendors or third parties engaged in this hardware, application, or service and pertain to relevant security practices and procedures.

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
A1	DC	Does the solution require user authentication, and does that authentication solution support OpenID Connect or OAUTH2 to provide single sign-on?				
A2	DC TEL x	Will the system provide internet security functionality on public portals using encrypted network/secure socket layer connections in line with current recommendations of the Open Web Application Security Project (OWASP)?				

A3	POC	Will the system have role-based access?				
A4	DC TEL	Does the application contain mitigations for risks associated to uncontrolled login attempts (response latency, re-Captcha, lockout, IP filtering, multi-factor authentication)? Which mitigations are in place? What are the optional mitigations?				
A5	DC TEL	Are account credentials hashed and encrypted when stored?				
A6	DC TEL x	The protection of the State's system and data is of upmost importance. Security scans must be done if: • An application will be placed on the State's system. • The State's system connects to another system. • The contractor hosts State data. • The contractor has another party host State data the State will want to scan that party. **The State would want to scan a test system; not a production system and will not do penetration testing.** The scanning will be done with industry standard tools. Scanning would also take place annually as well as when there are code changes. Are either of these an issue? If so, please explain.				
A7	DC	Will SSL traffic be decrypted and inspected before it is allowed into your system?				
A8	POC x	Will organizations other than the State of South Dakota have access to our data?				
A9	DEV TEL	Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?				
A10	DEV	Are there some requirements for security that are "structured" as part of general release readiness of a product, and others that are "as needed" or "custom" for a particular release?				
A11	TEL	What threat assumptions were made, if any, when designing protections for the software and information assets processed?				
A12	TEL	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?				
A13	TEL	What security criteria, if any, are considered when selecting third party suppliers?				

A14	TEL	How has the software been measured/assessed for its resistance to publicly known vulnerabilities and/or attack patterns identified in the Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumerations (CWEs)? How have the findings been mitigated?	▨	▨		
A15	TEL	Has the software been evaluated against the Common Criteria, FIPS 140-2, or other formal evaluation process? If so, please describe what evaluation assurance level (EAL) was achieved, what protection profile the product claims conformance to, and indicate if the security target and evaluation report are available.				
A16	DC TEL	Are static or dynamic software security analysis tools used to identify weaknesses in the software that can lead to exploitable vulnerabilities? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?				
A17	DC TEL x	Has the product undergone any vulnerability and/or penetration testing? If yes, how frequently, by whom, and are the test reports available under a nondisclosure agreement? How have the findings been mitigated?				
A18	DC	Does your company have an executive-level officer responsible for the security of your company's software products and/or processes?				
A19	DC	How are software security requirements developed?	▨	▨		
A20	DC	What risk management measures are used during the software's design to mitigate risks posed by use of third-party components?	▨	▨		
A21	DC	What is your background check policy and procedure? Are your background checks fingerprint based?				
A22	DEV	Does your company have formally defined security policies associated with clearly defined roles and responsibilities for personnel working within the software development life cycle? Explain.				
A23	TEL	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?	▨	▨		
A24	DC TEL	Do you have an automated Security Information and Event Management system?				

A25	DC TEL	What types of event logs do you keep and how long do you keep them?				
		a. System events				
		b. Application events				
		c. Authentication events				
		d. Physical access to your data center(s)				
		e. Code changes				
		f. Other:				
A26	DC	How are security logs and audit trails protected from tampering or modification? Are log files consolidated to single servers?				
A27	DEV	a. Are security specific regression tests performed during the development process?				
		b. If yes, how frequently are the tests performed?				
A28	TEL	What type of firewalls (or application gateways) do you use? How are they monitored/managed?				
A29	TEL	What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?				
A30	DC TEL	What are your procedures for intrusion detection, incident response, and incident investigation and escalation?				
A31	DC TEL	Do you have a BYOD policy that allows your staff to put any sort of sensitive or legally protected State data on their device personal device(s) or other non-company owned system(s)?				
A32	DC TEL	Do you require multifactor authentication be used by employees and subcontractors who have potential access to legally protected State data or administrative control? If yes, please explain your practices on multifactor authentication including the authentication level used as defined in NIST 800-63 in your explanation. If no, do you plan on implementing multifactor authentication? If so, when?				

A33	POC	Will this system provide the capability to track data entry/access by the person, date, and time?				
A34	DC DEV POC TEL	Will the system provide data encryption for sensitive or legally protected information both at rest and transmission? If yes, please provide details.				
A35	DC	a. Do you have a SOC 2 or ISO 27001 audit report?				
		b. Is the audit performed annually?				
		c. If it is SOC 2 audit report, does it cover all 5 of the trust principles?				
		d. If it is a SOC 2 audit report, what level is it?				
		e. Does the audit include cloud service providers?				
		f. Has the auditor always been able to attest to an acceptable audit result?				
		g. Will you provide a copy of your latest SOC 2 or ISO 27001 audit report upon request? A redacted version is acceptable.				
A36	DC	Do you or your cloud service provider have any other security certification beside SOC 2 or ISO 27001, for example, FedRAMP or ITTRUST?				
A37	DC TEL	Are you providing a device or software that can be defined as being Internet of Thing (IoT)? Examples include IP camera, network printer, or connected medical device. If yes, what is your process for ensuring the software on your IoT devices that are connected to the state's system, either permanently or intermittently, are maintained and/or updated?				
A38	DC	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?	▨	▨		
A39	DC	What are your policies and procedures for hardening servers?	▨	▨		
A40	DC TEL	**(Only to be used when medical devices are being acquired.)** Please give the history of cybersecurity advisories issued by you for your medical devices. Include the device, date, and the nature of the cybersecurity advisory.	▨	▨		

A41	DC POC	Does any product you propose to use or provide the State include software, hardware, or hardware components manufactured by any company on the US Commerce Department's Entity List?				
A42	DC	Describe your process for monitoring the security of your suppliers.				

Section B. Hosting

The following questions are relevant to any hosted applications, systems, databases, services, and any other technology. The responses should not assume a specific hosting platform, technology, or service but instead the response should address any hosting options available for the proposed solution.

For state-hosted systems that reside in a state-managed cloud:

To minimize impacts to project schedules, vendors are required to provide architectural plans, resource needs, permission plans, and all interfaces – both internal to the state and internet facing for cloud hosted systems. The documentation provided will be reviewed as part of the initial assessment process. If selected for award of a contract, and once the state has approved the submitted materials, a test environment will be provided after contract signature. Systems will be reviewed again before being moved to a production environment. Any usage or processes that are deemed out of compliance with what was approved or represent excessive consumption or risk will require remediation before being moved to production.

						Response
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
B1	POC	Are there expected periods of time where the application will be unavailable for use?				
B2	DC	If you have agents or scripts executing on servers of hosted applications what are the procedures for reviewing the security of these scripts or agents?				
B3	DC	What are the procedures and policies used to control access to your servers? How are audit logs maintained?				
B4	DC DEV POC TEL	Do you have a formal disaster recovery plan? Please explain what actions will be taken to recover from a disaster. Are warm or hot backups available? What are the Recovery Time Objectives and Recovery Point Objectives?				
B5	DC	Explain your tenant architecture and how tenant data is kept separately?				
B6	DC	What are your data backup policies and procedures? How frequently are your backup procedures verified?				
B7	DC DEV TEL	If any cloud services are provided by a third-party, do you have contractual requirements with them dealing with: • Security for their I/T systems; • Staff vetting; • Staff security training?				
		a. If yes, summarize the contractual requirements.				

		b. If yes, how do you evaluate the third-party's adherence to the contractual requirements?	▨	▨		
B8	DC	If your application is hosted by you or a third party, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal? If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?				
B9	DC	a. Do you use a security checklist when standing up any outward facing system?				
		b. Do you test after the system was stood up to make sure everything in the checklist was correctly set?				
B10	DC	How do you secure Internet of Things (IoT) devices on your network?	▨	▨		
B11	DC TEL	Do you use Content Threat Removal to extract and transform data?				
B12	DC TEL	Does your company have an endpoint detection and response policy?				
B13	DC TEL	Does your company have any real-time security auditing processes?				
B14	TEL	How do you perform analysis against the network traffic being transmitted or received by your application, systems, or data center? What benchmarks do you maintain and monitor your systems against for network usage and performance? What process(es) or product(s) do you use to complete this analysis, and what results or process(es) can you share?	▨	▨		
B15	TEL	How do you monitor your application, systems, and data center for security events, incidents, or information? What process(es) and/or product(s) do you use to complete this analysis, and what results or process(es) can you share?				
B16	DC TEL	What anti-malware product(s) do you use?	▨	▨		
B17	DC TEL	What is your process to implement new vendor patches as they are released and what is the average time it takes to deploy a patch?	▨	▨		
B18	DC TEL	Have you ever had a data breach? If so, provide information on the breach.				
B19	POC	Is there a strategy for mitigating unplanned disruptions and what is it?				
B20	DC TEL	What is your process for ensuring the software on your IoT devices that are connected to your system, either permanently or intermittently, is maintained and updated?	▨	▨		
B21	POC	Will the State of South Dakota own the data created in your hosting environment?				

B22	DEV	What are your record destruction scheduling capabilities?				

Section C: Database
The following questions are relevant to any application or service that stores data, irrespective of the application being hosted by the state or the vendor.

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
C1	DC	Will the system require a database?				
C2	DC	If a Database is required, what technology will be used (i.e. Microsoft SQL Server, Oracle, MySQL)?				
C3	DC	If a SQL Database is required does the cost of the software include the cost of licensing the SQL Server?				
C4	POC	Will the system data be exportable by the user to tools like Excel or Access at all points during the workflow?				
C5	DC DEV	Will the system infrastructure include a separate OLTP or Data Warehouse Implementation?				
C6	DC DEV	Will the system infrastructure require a Business Intelligence solution?				

Section D: Contractor Process
The following questions are relevant for all vendors or third parties engaged in providing this hardware, application, or service and pertain to business practices. If the application is hosted by the vendor or the vendor supplies cloud services those questions dealing with installation or support of applications on the State's system can be marked "NA".

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
D1	DC POC	Will the vendor provide assistance with installation?				
D2	DC DEV POC TEL	Does your company have a policy and process for supporting/requiring professional certifications? If so, how do you ensure certifications are valid and up-to date?				
D3	DEV	What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing, and integrated testing)?				
D4	DEV	Are misuse test cases included to exercise potential abuse scenarios of the software?				
D5	TEL	What release criteria does your company have for its products regarding security?				
D6	DEV	What controls are in place to ensure that only the accepted/released software is placed on media for distribution?				
D7	DC DEV	a. Is there a Support Lifecycle Policy within the organization for the software				
		b. Does it outline and establish a consistent and predictable support timeline?				

D8	DC	How are patches, updates, and service packs communicated and distributed to the State?				
D9	DEV	What services does the help desk, support center, or (if applicable) online support system offer when are these services available, and are there any additional costs associated with the options?				
D10	DC	a. Can patches and service packs be uninstalled?				
		b. Are the procedures for uninstalling a patch or service pack automated or manual?				
D11	DC DEV	How are enhancement requests and reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, prioritized, and reported? Is the management and reporting policy available for review?				
D12	DC	What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches, updates, and service packs?				
D13	DC	Are third-party developers contractually required to follow your configuration management and security policies and how do you assess their compliance?				
D14	DEV	What policies and processes does your company use to verify that your product has its comments sanitized and does not contain undocumented functions, test/debug code, or unintended, “dead,” or malicious code? What tools are used?				
D15	DEV	How is the software provenance verified (e.g., any checksums or signatures)?				
D16	DEV	a. Does the documentation explain how to install, configure, and/or use the software securely?				
		b. Does it identify options that should not normally be used because they create security weaknesses?				
D17	DEV	a. Does your company develop security measurement objectives for all phases of the SDLC?				
		b. Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security measures?				
D18	DC	a. Is testing done after changes are made to servers?				
		b. What are your rollback procedures in the event of problems resulting from installing a patch or service pack?				

D19	DC	What are your procedures and policies for handling and destroying sensitive data on electronic and printed media?				
D20	DC TEL	How is endpoint protection done? For example, is virus prevention used and how are detection, correction, and updates handled?				
D21	DC TEL	Do you perform regular reviews of system and network logs for security issues?				
D22	DC	Do you provide security performance measures to the customer at regular intervals?				
D23	DC POC	What technical, installation, and user documentation do you provide to the State? Is the documentation electronically available and can it be printed?				
D24	DC DEV POC	a. Will the implementation plan include user acceptance testing?				
		b. If yes, what were the test cases?				
		c. Do you do software assurance?				
D25	DC DEV POC TEL	Will the implementation plan include performance testing?				
D26	DEV POC	Will there be documented test cases for future releases including any customizations done for the State of South Dakota?				
D27	DEV POC	If the State of South Dakota will gain ownership of the software, does the proposal include a knowledge transfer plan?				
D28	DEV POC	Has your company ever conducted a project where your product was load tested?				
D29	DC	Please explain the pedigree of the software. Include in your answer who are the people, organization, and processes that created the software.				
D30	DC	Explain the change management procedure used to identify the type and extent of changes allowed in the software throughout its lifecycle. Include information on the oversight controls for the change management procedure.				
D31	DC DEV TEL	Does your company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? **Provide a brief explanation**. Will the supplier indemnify the acquirer from these issues in the license agreement? **Provide a brief explanation.**				
D32	DEV	Summarize the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers),				

		techniques, etc. used to produce and transform the software.				
D33	DEV	a. Does the software contain third-party developed components?				
		b. If yes, are those components scanned by a static code analysis tool?				
D34	DC DEV TEL	What security design and security architecture documents are prepared as part of the SDLC process? How are they maintained? Are they available to/for review?				
D35	DEV	Does your organization incorporate security risk management activities as part of your software development methodology? If yes, please provide a copy of this methodology or provide information on how to obtain it from a publicly accessible source.				
D36	DC	Does your company ever perform site inspections/policy compliance audits of its U.S. development facilities? Of its non-U.S. facilities? Of the facilities of its third-party developers? If yes, how often do these inspections/audits occur? Are they periodic or triggered by events (or both)? If triggered by events, provide examples of "trigger" events.				
D37	DC TEL	How are trouble tickets submitted? How are support issues, specifically those that are security-related escalated?				
D38	DC DEV	Please describe the scope and give an overview of the content of the security training you require of your staff, include how often the training is given and to whom. Include training specifically given to your developers on secure development.				
D39	DC TEL x	It is State policy that all Contractor Remote Access to systems for support and maintenance on the State Network will only be allowed through Citrix Netscaler. Would this affect the implementation of the system?				
D40	POC TEL x	Contractors are also expected to reply to follow-up questions in response to the answers they provided to the security questions. At the State's discretion, a contractor's answers to the follow-up questions may be required in writing and/or verbally. The answers provided may be used as part of the contractor selection criteria. Is this acceptable?				
D41	DC DEV POC TEL x	(For PHI only) a. Have you done a risk assessment? If yes, will you share it?				

		b. If you have not done a risk assessment, when are you planning on doing one?				
		c. If you have not done a risk assessment, would you be willing to do one for this project?				
D42	DEV POC	Will your website conform to the requirements of Section 508 of the Rehabilitation Act of 1973?				

Section E: Software Development
The following questions are relevant to the tools and third-party components used to develop your application, irrespective of the application being hosted by the State or the vendor.

						Response
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed.**
E1	DEV POC x	What are the development technologies used for this system? Please indicate version as appropriate.				
		ASP.Net				
		VB.Net				
		C#.Net				
		.NET Framework				
		Java/JSP				
		MS SQL				
		Other				
E2	DC TEL	Is this a browser-based user interface?				
E3	DEV POC	Will the system have any workflow requirements?				
E4	DC	Can the system be implemented via Citrix?				
E5	DC	Will the system print to a Citrix compatible networked printer?				
E6	TEL	If your application does not run under the latest Microsoft operating system, what is your process for updating the application?				
E7	DEV	Identify each of the Data, Business, and Presentation layer technologies your product would use and provide a roadmap outlining how your release or update roadmap aligns with the release or update roadmap for this technology.				
E8	TEL x	Will your system use Adobe Air, Adobe Flash, Adobe ColdFusion, Apache Flex, Microsoft Silverlight, PHP, Perl, Magento, or QuickTime? If yes, explain?				
E9	DEV	To connect to other applications or data, will the State be required to develop custom interfaces?				
E10	DEV	To fulfill the scope of work, will the State be required to develop reports or data extractions from the database? Will you provide any APIs that the State can use?				
E11	DEV POC	Has your company ever integrated this product with an enterprise service bus to exchange data between diverse computing platforms?				

E12	DC	a. If the product is hosted at the State, will there be any third-party application(s) or system(s) installed or embedded to support the product (for example, database software, run libraries)?				
		b. If yes, please list those third-party application(s) or system(s).	▨	▨		
E13	DEV	What coding and/or API standards are used during development of the software?				
E14	DEV	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?				
E15	DEV	How does the software's exception handling mechanism prevent faults from leaving the software, its resources, and its data (in memory and on disk) in a vulnerable state?	▨	▨		
E16	DEV	Does the exception handling mechanism provide more than one option for responding to a fault? If so, can the exception handling options be configured by the administrator or overridden?				
E17	DEV	What percentage of code coverage does your testing provide?	▨	▨		
E18	DC	a. Will the system infrastructure involve the use of email?				
		b. Will the system infrastructure require an interface into the State's email infrastructure?				
		c. Will the system involve the use of bulk email distribution to State users? Client users? In what quantity will emails be sent, and how frequently?				
E19	TEL x	a. Does your application use any Oracle products?				
		b. If yes, what product(s) and version(s)?	▨	▨		
		c. Do you have support agreements for these products?				
E20	DC	Explain how and where the software validates (e.g., filter with whitelisting) inputs from untrusted sources before being used.	▨	▨		
E21	TEL	a. Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user)?				
		b. Is it designed to isolate and minimize the extent of damage possible by a successful attack?				
E22	TEL	Does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?				
E23	TEL	If your application will be running on a mobile device, what is your process for making sure your				

		application can run on the newest version of the mobile device’s operating system?				
E24	DEV	Do you use open-source software or libraries? If yes, do you check for vulnerabilities in your software or library that are listed in:				
		a. Common Vulnerabilities and Exposures (CVE) database?				
		b. Open-Source Vulnerability Database (OSVDB)?				
		c. Open Web Application Security Project (OWASP) Top Ten?				

F. Infrastructure
The following questions are relevant to how your system interacts with the State’s technology infrastructure. If the proposed technology does not interact with the State’s system, the questions can be marked “NA”.

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed.**
F1	DC	Will the system infrastructure have a special backup requirement?				
F2	DC	Will the system infrastructure have any processes that require scheduling?				
F3	DC	The State expects to be able to move your product without cost for Disaster Recovery purposes and to maintain high availability. Will this be an issue?				
F4	TEL x	Will the network communications meet Institute of Electrical and Electronics Engineers (IEEE) standard TCP/IP (IPv4, IPv6) and use either standard ports or State-defined ports as the State determines?				
F5	DC x	It is State policy that all systems must be compatible with BIT’s dynamic IP addressing solution (DHCP). Would this affect the implementation of the system?				
F6	TEL x	It is State policy that all software must be able to use either standard Internet Protocol ports or Ports as defined by the State of South Dakota BIT Network Technologies. Would this affect the implementation of the system? If yes, explain.				
F7	DC	It is State policy that all HTTP/SSL communication must be able to be run behind State of South Dakota content switches and SSL accelerators for load balancing and off-loading of SSL encryption. The State encryption is also PCI compliant. Would this affect the implementation of your system? If yes, explain.				
F8	DC x	The State has a virtualize first policy that requires all new systems to be configured as virtual machines. Would this affect the implementation of the system? If yes, explain.				

F9	TEL x	It is State policy that all access from outside of the State of South Dakota's private network will be limited to set ports as defined by the State and all traffic leaving or entering the State network will be monitored. Would this affect the implementation of the system? If yes, explain.				
F10	TEL	It is State policy that systems must support Network Address Translation (NAT) and Port Address Translation (PAT) running inside the State Network. Would this affect the implementation of the system? If yes, explain.				
F11	TEL x	It is State policy that systems must not use dynamic Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports unless the system is a well-known one that is state firewall supported (FTP, TELNET, HTTP, SSH, etc.). Would this affect the implementation of the system? If yes, explain.				
F12	DC	The State of South Dakota currently schedules routine maintenance from 0400 to 0700 on Tuesday mornings for our non-mainframe environments and once a month from 0500 to 1200 for our mainframe environment. Systems will be offline during this scheduled maintenance time periods. Will this have a detrimental effect to the system?				
F13	POC TEL	Please describe the types and levels of network access your system/application will require. This should include, but not be limited to TCP/UDP ports used, protocols used, source and destination networks, traffic flow directions, who initiates traffic flow, whether connections are encrypted or not, and types of encryption used. The Contractor should specify what access requirements are for user access to the system and what requirements are for any system level processes. The Contractor should describe all requirements in detail and provide full documentation as to the necessity of the requested access.				
F14	POC x	List any hardware or software you propose to use that is not State standard, the standards can be found at http://bit.sd.gov/standards/.				
F15	DC	Will your application require a dedicated environment?				
F16	DEV POC	Will the system provide an archival solution? If not, is the State expected to develop a customized archival solution?				
F17	DC TEL	Provide a system diagram to include the components of the system, description of the component, and how the components communicate with each other.				

F18	DC	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?				
F19	TEL x	It is State policy that no equipment can be connected to State Network without direct approval of BIT Network Technologies. Would this affect the implementation of the system?				
F20	DC x	Will the server-based software support: a. Windows server 2016 or higher				
		b. IIS7.5 or higher				
		c. MS SQL Server 2016 standard edition or higher				
		d. Exchange 2016 or higher				
		e. Citrix XenApp 7.15 or higher				
		f. VMWare ESXi 6.5 or higher				
		g. MS Windows Updates				
		h. Carbon Black				
F21	TEL x	All network systems must operate within the current configurations of the State of South Dakota's firewalls, switches, IDS/IPS, and desktop security infrastructure. Would this affect the implementation of the system?				
F22	DC	All systems that require an email interface must use SMTP Authentication processes managed by BIT Datacenter. Mail Marshal is the existing product used for SMTP relay. Would this affect the implementation of the system?				
F23	DC TEL	The State implements enterprise-wide anti-virus solutions on all servers and workstations as well as controls the roll outs of any and all Microsoft patches based on level of criticality. Do you have any concerns regarding this process?				
F24	DC TEL	What physical access do you require to work on hardware?				
F25	DC	How many of the vendor's staff and/or subcontractors will need access to the state system, will this be remote access, and what level of access will they require?				

Section G: Business Process
The following questions pertain to how your business model interacts with the State's policies, procedures, and practices. If the vendor is hosting the application or providing cloud services, questions dealing with installation or support of applications on the State's system can be marked "NA".

						Response
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed.**
G1	DC	a. If your application is hosted on a dedicated environment within the State's infrastructure, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal?				

		b. If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?				
G2	POC	Explain the software licensing model.	▨	▨		
G3	DC DEV POC	Is on-site assistance available? If so, what is the charge?				
G4	DEV POC	a. Will you provide customization of the system if required by the State of South Dakota?				
		b. If yes, are there any additional costs for the customization?				
G5	POC	Explain the basis on which pricing could change for the State based on your licensing model.	▨	▨		
G6	POC	Contractually, how many years price lock will you offer the State as part of your response? Also, as part of your response, how many additional years are you offering to limit price increases and by what percent?	▨	▨		
G7	POC	Will the State acquire the data at contract conclusion?				
G8	POC	Will the State's data be used for any other purposes other than South Dakota's usage?				
G9	DC	Has your company ever filed for Bankruptcy under U.S. Code Chapter 11? If so, please provide dates for each filing and describe the outcome.				
G10	DC	Has civil legal action ever been filed against your company for delivering or failing to correct defective software? Explain.				
G11	DC	Please summarize your company's history of ownership, acquisitions, and mergers (both those performed by your company and those to which your company was subjected).	▨	▨		
G12	DC	Will you provide on-site support 24x7 to resolve security incidents? If not, what are your responsibilities in a security incident?				
G13	DEV	What training programs, if any, are available or provided through the supplier for the software? Do you offer certification programs for software integrators? Do you offer training materials, books, computer-based training, online educational forums, or sponsor conferences related to the software?	▨	▨		
G14	DC TEL	Are help desk or support center personnel internal company resources or are these services outsourced to third parties? Where are these resources located?	▨	▨		
G15	DC	Are any of the services you plan to use located offshore (examples include data hosting, data processing, help desk, and transcription services)?				

G16	DC	Is the controlling share (51%+) of your company owned by one or more non-U.S. entities?				
G17	DC	What are your customer confidentiality policies? How are they enforced?	▨	▨		
G18	DC POC x	Will this application now or possibly in the future share PHI with other entities on other networks, be sold to another party or be accessed by anyone outside the US?				
G19	DC	If the product is hosted at the State, will there be a request to include an application to monitor license compliance?				
G20	DC POC	Is telephone assistance available for both installation and use? If yes, are there any additional charges?				
G21	DC TEL	What do you see as the most important security threats your industry faces?	▨	▨		